Global Investigations Review

The Practitioner's Guide to Global Investigations

Volume I: Global Investigations in the United Kingdom and the United States

Fourth Edition

Editors
Judith Seddon, Eleanor Davison, Christopher J Morvillo,
Michael Bowes QC, Luke Tolaini, Ama A Adams, Tara McGrath

2020

The Practitioner's Guide to Global Investigations

Fourth Edition

Editors

Judith Seddon

Eleanor Davison

Christopher J Morvillo

Michael Bowes QC

Luke Tolaini

Ama A Adams

Tara McGrath

GIR

Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of November 2019, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: natalie.hacker@lbresearch.com
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-228-2

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Dedicated to the memory of Rod Fletcher, one of the United Kingdom's most highly respected white-collar crime lawyers and a cherished friend.

Acknowledgements

ADDLESHAW GODDARD LLP
ALLEN & OVERY LLP
ANAGNOSTOPOULOS
ASSOCIATION OF CORPORATE INVESTIGATORS
BAKER MCKENZIE LLP
BCL SOLICITORS LLP
BDO USA, LLP
BOFILL MIR & ALVAREZ JANA
BORDEN LADNER GERVAIS LLP
BROWN RUDNICK LLP
BRUNSWICK GROUP LLP
CADWALADER, WICKERSHAM & TAFT LLP
CLIFFORD CHANCE
CLOTH FAIR CHAMBERS
CMS CAMERON MCKENNA NABARRO OLSWANG LLP SCP
CONOR REARDON ESQ
CORKER BINNING
CRAVATH, SWAINE & MOORE LLP
DEBEVOISE & PLIMPTON LLP
DECHERT LLP
DLA PIPER LLP
FORNARI E ASSOCIATI
FOUNTAIN COURT CHAMBERS
FOX WILLIAMS LLP
FRESHFIELDS BRUCKHAUS DERINGER

GLEISS LUTZ

GOODWIN

GÜN + PARTNERS

HERBERT SMITH FREEHILLS LLP

HOMBURGER

JAMES P LOONAM ESQ

JENNER & BLOCK LLP

KINGSLEY NAPLEY LLP

KNOETZL

LATHAM & WATKINS

LAW OFFICES OF PANAG AND BABU

LINKLATERS LLP

MARVAL O'FARRELL & MAIRAL

MATHESON

MATRIX CHAMBERS

MILLER & CHEVALIER CHARTERED

NAVACELLE

OUTER TEMPLE CHAMBERS

PHILIPPI PRIETOCARRIZOSA FERRERO DU & URÍA – PPU

PINSENT MASONS LLP

RAJAH & TANN SINGAPORE LLP

REBAZA, ALCÁZAR & DE LAS CASAS

REED SMITH LLP

ROPES & GRAY LLP

RUSSELL MCVEAGH

SKADDEN, ARPS, SLATE, MEAGHER & FLOM (UK) LLP

SLAUGHTER AND MAY

SOFUNDE OSAKWE OGUNDIPE & BELGORE

SULLIVAN & CROMWELL LLP

TRENCH ROSSI WATANABE

VON WOBESER Y SIERRA, SC

WALDEN MACHT & HARAN LLP

Publisher's Note

The Practitioner's Guide to Global Investigations is published by Global Investigations Review (www.globalinvestigationsreview.com) – a news and analysis service for lawyers and related professionals who specialise in cross-border white-collar crime.

The Guide was suggested by the editors to fill a gap in the literature – namely, how does one conduct such an investigation, and what should one have in mind at various times?

It is published annually as a two-volume work and is also available online, as an e-book and in PDF format.

The volumes

This Guide is in two volumes.

Volume I takes the reader through the issues and risks faced at every stage in the life cycle of a serious corporate investigation, from the discovery of a potential problem through its exploration (either by the company itself, a law firm or government officials) all the way to final resolution – be that in a regulatory proceeding, a criminal hearing, civil litigation, an employment tribunal, a trial in the court of public opinion, or, just occasionally, inside the company's own four walls. As such it uses the position in the two most active jurisdictions for investigations of corporate misfeasance – the United States and the United Kingdom – to illustrate the approach and thought processes of those who are at the cutting edge of this work, on the basis that others can learn much from their approach, and there is a read-across to the position elsewhere.

Volume I is then complemented by Volume II's granular look at the detail of various jurisdictions, highlighting, among other things, where they vary from the norm.

Online

The Guide is available at www.globalinvestigationsreview.com. Containing the most up-to-date versions of the chapters in Volume I of the Guide, the website also allows visitors to quickly compare answers to questions in Volume II across all the jurisdictions covered.

The publisher would like to thank the editors for their exceptional energy, vision and intellectual rigour in devising and maintaining this work. Together we welcome any comments or suggestions from readers on how to improve it. Please write to us at:
insight@globalinvestigationsreview.com.

Preface

The history of the global investigation

Over the past decade, the number and profile of multi-agency, multi-jurisdictional regulatory and criminal investigations have risen exponentially. Naturally, this global phenomenon exposes companies and their employees to greater risk of potentially hostile encounters with foreign law enforcement authorities and regulators than ever before. This is partly owing to the continued globalisation of commerce, the increasing enthusiasm of some prosecutors to use expansive theories of corporate criminal liability to exact exorbitant penalties against corporations as a deterrent and public pressure to hold individuals accountable for the misconduct. The globalisation of corporate law enforcement, of course, has also spawned greater coordination between law enforcement agencies domestically and across borders. As a result, the pace and complexity of cross-border corporate investigations has markedly increased and created an environment in which the potential consequences, both direct and collateral, for individuals and businesses are of unprecedented magnitude.

The Guide

To aid practitioners faced with the myriad and often unexpected challenges of navigating a cross-border investigation, this book brings together for the first time the perspectives of leading experts from across the globe.

The chapters that follow in Volume I of the Guide cover in depth the broad spectrum of the law, practice and procedure applicable to cross-border investigations in both the United Kingdom and United States. Volume I tracks the development of a serious allegation (whether originating from an internal or external source) through its stages of development, considering the key risks and challenges as matters progress; it provides expert insight into the fact-gathering stage, document preservation and collection, witness interviews, and the complexities of cross-border privilege issues; and it discusses strategies to successfully resolve cross-border probes and manage corporate reputation throughout an investigation.

In Volume II, local experts from national jurisdictions respond to a common set of questions designed to identify the local nuances of law and practice that practitioners may encounter in responding to a cross-border investigation.

In the first edition, we signalled our intention to update and expand both parts of the book as the rules evolve and prosecutors' appetites change. The Guide continues to grow and extend its reach, in both substance and geographical scope. By its third edition, it had outgrown its original single-book format; the two parts of the Guide now have separate covers, although the hard copy of the Guide should still be viewed – and used – as a single reference work. All chapters are, of course, made available online and in other digital formats. Volume I also features tables of cases and legislation along with an index.

In this fourth edition, we have revised extant chapters to keep up with recent developments. To reflect an increased prosecutorial focus on individual accountability and on tone at the top, we have added US and UK chapters on the duties of directors to Volume I, outlining quite divergent corporate governance models. The questionnaire for Volume II authors has been extensively revised and reviewed by the editors and GIR staff. New questions zero in on the growing importance of technology in carrying out and investigating misconduct. There are also questions on economic sanctions, an area of heightened enforcement activity, which GIR has responded to this year with the launch of Just Sanctions (https://globalinvestigationsreview.com/just-sanctions). Volume II also carries regional overviews giving insight into cultural issues and regional coordination by authorities.

Volume II covers 25 jurisdictions, increasing the global coverage, particularly in South America, which continues to rake over recent corruption scandals. As corporate investigations and enforcer co-operation crosses more borders, we anticipate Volume II will become increasingly valuable to our readers: external and in-house counsel; compliance and accounting professionals; and prosecutors and regulators operating in this complex environment.

Acknowledgements

The Editors gratefully acknowledge the insightful contributions of the following lawyers from Clifford Chance: Oliver Pegden in London, Amy Montour and Mary Jane Yoon in New York, and Hena Schommer and Michelle Williams in Washington, DC. The Editors would also especially like to thank Clifford Chance associate Kaitlyn Ferguson in Washington, DC, Chris Stott, senior attorney at Ropes & Gray LLP in London, and Zoe Osborne, partner at Steptoe & Johnson in London.

Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams, Tara McGrath
December 2019
London, New York and Washington, DC

Contents

Table of Cases

United Kingdom

United States of America

Australia

European Court of Human Rights

European Court of Justice

France

Hong Kong

New Zealand

Singapore

Table of Legislation

TABLE OF UK LEGISLATION

Statutes

Statutory Instruments

TABLE OF US LEGISLATION

CONSTITUTION

FEDERAL LEGISLATION

Federal Acts

US Code

Code of Federal Regulations (CFR)

Federal Rules

STATE LEGISLATION

Arizona:

California:

Connecticut:

Delaware:

District of Columbia:

Florida:

Illinois:

New York:

Ohio:

Oregon:

Pennsylvania:

Texas:

Washington:

TABLE OF OTHER NATIONAL LEGISLATION

Austria:

France:

Hong Kong:

Japan:

People's Republic of China:

Russia:

Switzerland:

TABLE OF INTERNATIONAL TREATIES, CONVENTIONS AND AGREEMENTS

TABLE OF EUROPEAN LEGISLATION

Treaties and Conventions

Regulations

Directives

Decisions

1

Introduction

Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams and Tara McGrath[1]

As an introduction to Volume I of the Guide, this chapter addresses UK and US law regarding two critical concepts that a company facing an investigation in either or both jurisdictions will often need to consider at the outset: corporate criminal liability and double jeopardy. This chapter also sets out in summary the priorities and challenges companies face at each stage of an investigation – topics that are explored in more detail in the chapters that follow. One topic not explored, but likely to affect chapters in this guide with a European dimension, is the United Kingdom's decision to leave the European Union. (At the time of writing, neither the date of any departure nor the precise basis on which any departure will occur is clear.) Considerable uncertainty still remains surrounding the consequences, legal and otherwise, of exit arrangements, which we hope will have become clearer by the next edition. Whatever the United Kingdom's relationship with the European Union, co-operation between UK and US law enforcement is likely only to increase.

Bases of corporate criminal liability 1.1

When corporate misconduct that potentially implicates multiple jurisdictions is uncovered, a critical preliminary question is: what is the test, in each jurisdiction, for corporate criminal liability? Not all countries have regimes for the criminal liability of companies, but for those jurisdictions that do, it typically rests on the premise that the acts of certain employees can be attributed to the corporation.

1 Judith Seddon and Ama A Adams are partners at Ropes & Gray LLP; Christopher J Morvillo and Luke Tolaini are partners, and Tara McGrath is a senior associate, at Clifford Chance; Eleanor Davison is a barrister at Fountain Court Chambers; and Michael Bowes QC is a barrister at Outer Temple Chambers.

However, the category of employees that can trigger corporate liability differs between jurisdictions – in some, it is limited to those with management responsibilities, whereas in others the category of employees who can trigger corporate liability is much broader. Generally speaking, the act triggering corporate liability must occur within the scope of the person's activities as an employee. The act must also generally be done in the interest of, or for the benefit of, the corporation. The difference between theories of liability across jurisdictions inevitably poses challenges and complicates a company's strategy for dealing with a global investigation, and in some instances can determine the outcome.

1.1.1 Corporate criminal liability in the United Kingdom

In the United Kingdom, there are two main techniques to attribute to a corporate the acts and states of mind of the individuals it employs.

The first is by use of the 'identification principle' – or identification doctrine – whereby, subject to some limited exceptions, a company may be held liable for the criminal acts of those who represent its directing mind and will, and who control what it does. The relevant test is set out in the leading case of *Tesco Ltd v. Nattrass*:

> *Where a limited company is the employer difficult questions do arise in a wide variety of circumstances in deciding which of its officers or servants is to be identified with the company so that his guilt is the guilt of the company.*
>
> *I must start by considering the nature of the personality which by a fiction the law attributes to a corporation. A living person has a mind which can have knowledge or intention or be negligent and he has hands to carry out his intentions. A corporation has none of these: it must act through living persons, though not always one or the same person. Then the person who acts is not speaking or acting for the company. He is acting as the company and his mind which directs his acts is the mind of the company. There is no question of the company being vicariously liable. He is not acting as a servant, representative, agent or delegate. He is an embodiment of the company or, one could say, he hears and speaks through the persona of the company, within his appropriate sphere, and his mind is the mind of the company. If it is a guilty mind then that guilt is the guilt of the company. It must be a question of law whether, once the facts have been ascertained, a person in doing particular things is to be regarded as the company or merely as the company's servant or agent.*[2]

2 *Tesco Supermarkets Ltd v. Nattrass* [1972] AC 153; reaffirmed in *Attorney General's Reference (No. 2 of 1999)* [2000] 2 Cr App R 207 at 217-218 in which Rose LJ stated: '*Tesco v. Nattrass* is still authoritative . . . and it is impossible to find a company guilty unless its alter ego is identified. None of the authorities since *Tesco v. Nattrass* . . . supports the demise of the doctrine of identification: all are concerned with statutory construction of different substantive offences and the appropriate rule of attribution was decided having regard to the legislative intent, namely whether Parliament intended companies to be liable. There is a sound reason for a special rule of attribution in relation to statutory offences rather than common law offences, namely there is, subject to a defence of reasonable practicability, an absolute duty imposed by the statutes. The authorities on statutory offences do not bear on the common law principle in relation to manslaughter. Lord Hoffmann's

It is for the judge to decide, as a matter of law, whether there is evidence on which a jury could be sure that a particular individual was a 'directing mind' within the *Tesco* principles; and, if there is such evidence, the jury must then be sure that the particular individual was in fact a directing mind for the purposes of his or her particular actions. A directing mind is not necessarily limited to board directors; it may also be found in a delegate who has full discretion to act independently of instructions from the directors. In short, under the identification principle, before a corporate can be found guilty of a criminal offence, someone who represents its directing mind and will must also be found guilty. There cannot be an aggregation of acts or omissions to attribute criminal conduct to the company; rather, the criminal act or omission must be performed by a single person who can be identified with the corporate for it to be liable.

The second technique of attributing liability to a company under English law is through vicarious liability. Although, in general, in the United Kingdom a corporate entity may not be convicted for the criminal acts of its inferior employees or agents, there are some exceptions, the most important of which concerns statutory offences that impose an absolute duty on the employer, even where the employer has not authorised or consented to the criminal act.[3]

Most significantly, statutory developments in the United Kingdom, starting with the offence of corporate manslaughter under the Corporate Manslaughter and Corporate Homicide Act 2007, but more significantly the introduction of the Bribery Act 2010 and more recently Part 3 of the Criminal Finances Act 2017, represent a policy shift by introducing the offences of failure to prevent by an 'associated person' committed on behalf of the company, unless the company can demonstrate that it had adequate (or reasonable) procedures in place to prevent such offences occurring. These statutes have broad jurisdictional reach. Under the Bribery Act, for example, a corporate falling within the definition of a commercial organisation could be guilty even where no conduct occurred in, and where the associated person has no connection with, the United Kingdom.

The policy of the legislation to improve corporate governance is clear: Ministry of Justice guidance for the Bribery Act refers to the need for a corporate to create

---

speech in Meridian is a re-statement not an abandonment of existing principles . . . .'; and *Environment Agency v. St Regis Paper Co. Ltd* [2012] 1 Cr App R 177 at paras. 10-12 in which, at para. 12, Moses LJ said: 'It seems to us that as a matter of statutory construction it is impossible to impose criminal liability for a breach . . . to the company in circumstances other than those where an intention to make a false entry can be attributed by operation of the rule in *Tesco Supermarkets*. There is, in our view, no warrant for imposing liability by virtue of the intentions of one who cannot be said to be the directing mind and will of [the defendant].' The identification principle was reaffirmed by the *Court of Appeal in R v. A Ltd, X, Y* [2016] EWCA Crim 1469. Most recently the Serious Fraud Office (SFO) was unsuccessful in having charges against Barclays Bank PLC reinstated through a voluntary bill of indictment, after all charges against the bank were dismissed in the Crown Court. The reasoning behind Davis LJ's decision cannot be reported until the conclusion of the trial of the individuals, including Barclays' former chief executive officer, https://www.sfo.gov.uk/2018/10/26/barclays-plc-and-barclays-bank-plc/.

3 These statutory offences are referred to by Rose LJ in *Attorney General's Reference (No. 2 of 1999)* [2000] 2 Cr App R 207 at 217-218, at footnote 2.

an 'anti-bribery culture'.[4] Similarly, a corporate is guilty of the offence of corporate manslaughter under the Corporate Manslaughter and Corporate Homicide Act 2007 if the way in which its activities are managed or organised causes a person's death where a duty of care was owed. Guidance issued for the corporate offences of failure to prevent the criminal facilitation of tax evasion, which closely mirrors the Bribery Act guidance, also refers to the culture of the organisation. For example, commitment from top-level management should foster 'a culture within the relevant body in which activity intended to facilitate tax evasion is never acceptable'.[5] Each piece of legislation and accompanying guidance invites consideration of the company's culture – its attitudes, policies, systems and practices. The test for liability is closer to the test in the regulatory context where liability is based on broad principles and considers governance, and systems and controls.

It may be that this model of corporate criminal liability expands, in due course, to all economic crimes; on 13 January 2017 the government issued a Call for Evidence (which concluded in March 2017) to examine whether the law on corporate criminal liability in the United Kingdom needs reform. The government said that it was seeking to establish whether there is evidence of corporate crime going unpunished because of the current impediments presented by the identification doctrine, as well as evidence on the costs and benefits of further reform, bearing in mind the significant changes made in certain sectors to tackle misconduct. This, it indicated, would inform government decisions over whether to make further reforms.[6] It set out five options for reform: amendment of the identification doctrine; a strict (vicarious) liability doctrine; a strict (direct) liability offence – effectively a widening of the current offence under section 7 of the UK Bribery Act (section 7 offence); incorporation of the failure-to-prevent wording into substantive offences, but with the burden on the prosecution to establish that the company had not taken adequate steps to prevent the unlawful conduct; and possible sector-by-sector regulatory reform (implementation in other sectors of arrangements similar to the new individual accountability regimes introduced for financial services). It is yet to be seen what impact political uncertainty in the United Kingdom will have on this thinking and whether the government decides to make fundamental changes once the more immediate challenges arising from the departure from the European Union have been addressed.

There are signs that there may be broad support for applying the approach taken with the section 7 offence to other economic offences. The clearest indication of this to date has been in the report published in March 2019 by a committee of the House of Lords examining the effectiveness of the UK Bribery Act. Reflecting evidence received from lawyers, NGOs and enforcement authorities

4 Ministry of Justice Guidance on the Bribery Act 2010, issued pursuant to section 9 of the Bribery Act 2010.

5 Her Majesty's Revenue and Customs, Tackling tax evasion: Government guidance for the corporate offence of failure to prevent the criminal facilitation of tax evasion, 1 September 2017, at p. 25.

6 Ministry of Justice, Corporate Liability for Economic Crime: Call for Evidence, Consultation Document, at p. 4.

(including on the practical challenges presented by the identification principle), it concluded that the section 7 offence is an effective tool and called on the UK government to expedite the decision on whether to apply the approach to other offences.[7]

In the deferred prosecution agreement (DPA) context, the current high threshold for establishing corporate criminal liability in the United Kingdom is a problem inherent in the DPA regime: to enter into a DPA, a prosecutor must satisfy the evidential test, which requires either that the evidential stage of the Full Code Test in the Code for Crown Prosecutors is satisfied,[8] or that:

> *there is at least a reasonable suspicion based upon some admissible evidence that [the company] has committed the offence, and there are reasonable grounds for believing that a continued investigation would provide further admissible evidence within a reasonable period of time, so that all the evidence together would be capable of establishing a realistic prospect of conviction in accordance with the Full Code Test.*[9]

For that reason many expected DPAs to be used principally for section 7 offences, where the identification principle does not present an obstacle to satisfying the evidential test. So too is the prospect of DPAs being used for the failure to prevent the facilitation of tax evasion offence specifically laid out in the government's guidance.[10] With all that said, two of the five DPAs concluded to date relate to fraud offences (*Tesco Stores Ltd*[11] and *Serco Geografix Ltd*[12]) where both sides of the negotiation have had to grapple with the identification principle and the need for agreement on the existence of a 'directing mind and will'. To some extent this has also been the case in two of the three DPAs concerned with bribery. Sarclad Limited,[13] in addition to section 7 culpability, also accepted primary liability in relation to conspiracies to corrupt and to bribe. Sarclad was, however, a small company and, as Sir Brian Leveson, then President of the Queen's Bench Division, found, 'there is no question but that [Sarclad] spiralled into criminality

7 House of Lords Bribery Act 2010 Committee, Bribery Act 2010 Post-legislative Scrutiny, report published 14 March 2019 (https://publications.parliament.uk/pa/ld201719/ldselect/ldbribact/303/30302.htm).

8 Namely that prosecutors must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction against each suspect on each charge. They must consider what the defence case may be, and how it is likely to affect the prospects of conviction. A case that does not pass the evidential stage must not proceed, no matter how serious or sensitive it may be.

9 DPA Code of Practice at para. 1.2(i)(b) (https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/deferred-prosecution-agreements/).

10 Her Majesty's Revenue and Customs, Tackling tax evasion: Government guidance for the corporate offence of failure to prevent the criminal facilitation of tax evasion, 1 September 2017, at p. 13.

11 *SFO v. Tesco Stores Ltd* [2019] Lloyd's Rep FC 283.

12 *SFO v. Serco Geografix Ltd* [2019] 7 WLUK 45.

13 Sarclad Limited was previously referred to as XYZ Limited pending the conclusion of associated proceedings against individuals. Those proceedings concluded with the acquittal of individuals in July 2019.

as a result of the conduct of a small number of senior executives bending to the will of agents.'[14] In other words, the identification principle did not, in that case, present a problem. However, in *Rolls-Royce*, the DPA spanned three decades, and dealt with conduct much of which pre-dated the introduction of the Bribery Act 2010 and which formed the basis of seven counts of conspiracy to corrupt and false accounting. The remaining five counts related to section 7 offences. We can conclude that in that case, despite being considerably larger than *Sarclad*, the identification principle did not present evidential hurdles in reaching a settlement although the Serious Fraud Office (SFO) closed its related investigation of individuals.

The Call for Evidence recognised that 'the effectiveness of the DPA as an alternative disposal depends on there being a realistic threat of prosecution', which, they conclude, 'lends weight to the suggestion that the "failure to prevent" model would offer a more realistic threat of successful prosecution than a case built on the application of the identification doctrine'.[15] The failure-to-prevent model as enacted in the Bribery Act and now the Criminal Finances Act is described in the Call for Evidence as having 'some clear advantages'. Apart from being readily applicable to offending by organisations of any size, the government is explicit in the power of the model to effect corporate cultural change by acting as 'an incentive to companies to include the prevention of economic crime as an integral part of corporate governance and, should it afford a more realistic threat of prosecution, it might enhance the effectiveness of DPAs as an alternative to criminal prosecution'.[16]

1.1.2 Corporate criminal liability in the United States

The United States has long recognised principles of corporate liability based on common law and statutory bases.[17] The application of these concepts, however, has evolved over time and was most recently shaped by the global financial crisis of 2007–2008, where the spectre of industry and market collapse loomed large. Today, increasing emphasis on individual liability and corporate culture continues to shape and refine this area of law.

In the United States, the common law of agency plays an important role. Specifically, under principles of *respondeat superior*, a company may be held vicariously liable for the illegal acts of any of its agents (including employees and contract personnel) so long as those actions were within the scope of the agents' duties and were intended, even if only in part, to benefit the corporation.[18] An act is considered 'within the scope of an agent's employment' if the individual commits

14 *SFO v. XYZ Ltd* (Case No. U20150856) (Preliminary Redacted) Approved Judgment, dated 8 July 2016 at para. 34.

15 Ministry of Justice, Corporate Liability for Economic Crime: Call for Evidence, Consultation Document, at p. 23.

16 Ibid. at p. 21.

17 Charles Doyle, Congressional Research Service, Corporate Criminal Liability: An Overview of Federal Law 1 (2013).

18 *Jones v. Federated Fin. Reserve Corp*., 144 F.3d 961, 965 (6th Cir. 1998). See also *Hamilton v. Carell*, 243 F.3d 992, 1001 (6th Cir. 2001).

the act as part of his or her general line of work and with at least the partial intent to benefit the corporation.[19] The corporation need not receive an actual benefit and may be liable for these offences even if it directs its agent not to commit the offence.[20]

Moreover, even where no single employee has the requisite intent or knowledge to satisfy the *scienter* element of a crime, courts have recognised a 'collective knowledge doctrine' – where several employees collectively know enough to satisfy the intent or knowledge requirement, courts can impute this collective intent and knowledge to the corporation.[21] While historically courts have used the doctrine to establish knowledge on the part of a corporation, in recent years the doctrine has also been used to establish a corporation's intent (i.e., to establish whether the corporation acted wilfully).[22] This doctrine is not universally accepted and some courts have limited it to circumstances where the company was flagrantly indifferent to the offences being committed.[23]

Additionally, beyond the common law principle of *respondeat superior*, some legislation imposes criminal liability for companies, including in the fields of environmental and antitrust law.[24] Such statutes have the dual effects of forcing companies to internalise the costs of their wrongdoing and of increasing the deterrent effect of the law or regulation. For example, in a field such as environmental law, where misconduct can have tremendous collateral and long-term consequences,

19 *United States v. Singh*, 518 F.3d 236, 249 (4th Cir. 2008) (citing *United States v. Automated Med. Labs.*, 770 F. 2d 399, 406–47 (4th Cir. 1985)).

20 *Automated Med. Labs.*, 770 F.2d at 407.

21 *United States v. Sci. Applications Int'l Corp.*, 555 F. Supp. 2d 40, 55–56 (D.C. Cir. 2008). See also *United States v. Bank of New England, N.A.*, 821 F.2d 844, 856 (1st Cir. 1987); *United States v. T.I.M.E.-D.C., Inc.*, 381 F. Supp. 730, 738–39 (W.D. Va. 1974).

22 See *United States v. Pac. Gas & Elec. Co.*, No. 14-CR-00175-TEH, 2015 WL 9460313 (N.D. Cal. 23 December 2015). There, a grand jury charged the Pacific Gas & Electric Company with violating the Pipeline Safety Act after a gas line erupted causing several deaths and injuries. The company moved to dismiss on the basis that the grand jury received incorrect instructions on, *inter alia*, collective intent. In denying the motion to dismiss, the court held that the collective knowledge of the corporation's employees demonstrated that they wilfully disregarded their legal duty to abide by the safety standards outlined in the Act. Id. at *3. Following a jury conviction on five counts, the company sought to have the case set aside; however, the court held that a reasonable juror could have found wilfulness beyond a reasonable doubt based on the evidence presented. *United States v. Pac. Gas & Elec. Co.*, No. 14-CR-00175-TEH, 2016 WL 6804575, at *3 (N.D. Cal. 17 November 2016). See also *United States v. FedEx Corp.*, 2016 U.S. Dist LEXIS 52438 (N.D. Cal. 18 April 2016) (denying FedEx's motion to dismiss, which was premised on the ground that the jury received incorrect instructions on collective intent and collective knowledge).

23 *T.I.M.E.-D.C., Inc.*, 381 F. Supp. at 740.

24 See, e.g., *United States v. Hopkins*, 53 F.3d 533 (2d Cir. 1995) (imposing a strict liability standard for a violation of the Clean Water Act); *United States v. Weitzenhoff*, 35 F.3d 1275 (9th Cir. 1993). *Contra United States v. Ahmad*, 101 F.3d 386 (5th Cir. 1996) (suggesting that there is a *mens rea* requirement for violations of the Clean Water Act). See also James Swann and Alex Ruoff, Self-Referral Law Seen as Barrier to New Provider Agreements, Bloomberg BNA (5 May 2016), http://www.bna.com/selfreferral-law-seen-n57982070764/ (discussing the physician self-referral law's imposition of strict liability).

the imposition of liability on the company acts as a strong incentive for corporate monitoring of employees and thorough due diligence and risk assessment.

Although corporate criminal liability has been a feature of US law since the nineteenth century,[25] the criminal prosecution of corporations slowed abruptly and significantly – although temporarily – following the ill-fated prosecution of Arthur Andersen in 2002; the conviction (subsequently overturned by the US Supreme Court) resulted in the firm's collapse and job losses for many thousands of innocent employees.[26] In the aftermath of the *Arthur Andersen* case, prosecutors became far more hesitant to unleash the brute force of criminal charges against companies.[27] Although limited prosecutions continued following *Arthur Andersen*, they were further reduced in number when, in the wake of the financial meltdown of 2007–2008, many feared that prosecuting big banks and large employers might lead to further economic turmoil.[28] This idea, that an entity might be 'too big to fail', is now widely rejected by both prosecutors and the public, and there has since been a marked uptick in prosecutions. Today, prosecutors are generally less willing to accept the prospect of dire collateral consequences as justification for not pursuing criminal charges against corporations and have required guilty pleas from large corporations, previously considered 'too big to jail'. As corporations survive – and even thrive – in the wake of guilty pleas, the spectre of the *Arthur Andersen* case recedes and the rigour with which prosecutors pursue companies continues to increase.[29]

In recent years, the United States has increasingly placed emphasis on an organisation's compliance culture and internal controls. The result is that self-reporting, full acceptance of responsibility and the disclosure of all relevant facts concerning culpable individuals (regardless of seniority) now form the basis on which the government awards co-operation credit. The Department of Justice's (DOJ) Justice Manual, the Security and Exchange Commission's (SEC) Seaboard factors, US Sentencing Guidelines and the 'Yates Memorandum', each of which is discussed in detail in later chapters, all reflect this pronounced shift in enforcement priorities. As a recent example, in late 2017 the DOJ introduced the Corporate

25 For a discussion of the history and development of corporate criminal liability in the United States, see Kathleen F Brickey, Corporate Criminal Accountability: A Brief History and an Observation, 60 Wash. U. L.Q. 393, 404–15 (1982).

26 *Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005). For a complete history of Arthur Andersen LLP, see Susan E Squires et al., *Inside Arthur Andersen: Shifting Values, Unexpected Consequences* (2003).

27 See Gabriel Markoff, 'Arthur Andersen and the Myth of the Corporate Death Penalty: Corporate Criminal Convictions in the Twenty-First Century', 15 U. Pa. J. Bus. L. 797, 805–07 (2013).

28 See Gretchen Morgenson and Louise Story, 'Behind the Gentler Approach to Banks by US', *N.Y. Times*, 7 July 2011, at A1.

29 See, e.g., Peter J Henning, 'Seeking Guilty Pleas From Corporations While Limiting the Fallout', N.Y. Times Dealbook (5 May 2014), https://dealbook.nytimes.com/2014/05/05/seeking-guilty-pleas-from-corporations-while-limiting-the-fallout/; Francine McKenna, 'Why the Ghost of Arthur Andersen No Longer Haunts Corporate Criminals', MarketWatch (21 May 2015), https://www.marketwatch.com/story/why-the-ghost-of-arthur-andersen-no-longer-haunts-corporate-criminals-2015-05-21.

Enforcement Policy, which creates a rebuttable presumption that the DOJ will grant a declination to a company in regard to Foreign Corrupt Practices Act (FCPA) violations where the company satisfies the requirements for voluntary self-disclosure, co-operation and remediation. The DOJ has also announced that it will use the Corporate Enforcement Policy as non-binding guidance in criminal cases outside the FCPA context.

Although the price of attaining corporate co-operation credit is often painfully high, most companies have no choice but to tolerate it; co-operation typically provides the best prospect for a company to prevent a criminal charge, minimise financial penalties and avoid other harsh collateral consequences, such as the imposition of a monitor. Still, co-operation is not for the faint of heart, and any company operating in the United States or subject to US jurisdiction should carefully consider the far-reaching consequences – both good and bad – of setting off down the often treacherous path of co-operation. Once a company voluntarily discloses misconduct to the government, the ability to defend the case and control the process is effectively relinquished, and a company will find it very difficult to withhold sensitive, embarrassing or even harmful information. Given the highly uncertain alternative to co-operation, however, most companies accept and embrace this new reality from the start of an internal investigation and understand that factual findings far more often than not – if they involve potential criminal misconduct – will be presented to law enforcement.[30]

Double jeopardy 1.2

Another key question in any global investigation – where misconduct crosses borders and where more than one enforcement authority may seek to assert jurisdiction – is the extent to which different authorities can sanction the same or similar conduct. While domestic constitutional provisions on double jeopardy are similar between nation states, no universally accepted international norm exists, and the protection afforded by the laws in one country may offer no protection in another. This can present a major difficulty to achieving a satisfactory global settlement for a client.

The doctrine of double jeopardy is that a person should not be tried twice for the same offence.[31] Its underlying objective is to bring finality to criminal proceedings against individuals and companies in specific circumstances. Double jeopardy applies to criminal proceedings, but has been held by the European Court of Human Rights (ECtHR) to encompass an administrative penalty, in circumstances where that penalty was classified as a criminal penalty because of the nature of the charges and the severity of the punishment.[32]

30 U.S. Dep't of Justice, Justice Manual §9-28.700 (2015).

31 The *ne bis in idem* or double jeopardy principle is well established both in EU law and under the European Convention on Human Rights. The phrase is derived from the Roman law maxim *nemo debet bis vexari pro una et eadem causa* (a man shall not be twice vexed [or tried] for the same cause).

32 *Grande Stevens and Others v. Italy* (4 March 2014) Application Nos. 18640/10, 18647/10, 18668/10 and 18698/10.

In the United Kingdom, there are two essential conditions for the doctrine to apply. First, the case must be 'finally disposed of' and second, any penalty imposed must actually have been enforced or be in the process of being enforced. The rationale for the doctrine is that it confers protection on the person (individual or corporate) from the risk of repeated prosecution by the State with its greater resources.[33] Reflecting similar concerns, the concept of double jeopardy in the United States is rooted in the Fifth Amendment to the US Constitution, which reads in relevant part: 'nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb'.[34] These twenty words have generated tens – if not hundreds – of thousands of pages of case law and are worthy of a treatise in themselves. Distilled to its essence, however, double jeopardy in the United States applies to prohibit subsequent prosecution or multiple punishments of an individual or corporation for the same conduct.[35] Nevertheless, the doctrine of double jeopardy is complicated by the question of dual sovereignty, which holds that double jeopardy's bar against successive prosecution for the same conduct does not apply when the prior prosecution was brought by a separate sovereign, for example, the US government is not barred from bringing a case where a state or another country has already prosecuted the defendant for the same conduct and *vice versa*.

1.2.1 Double jeopardy in the United Kingdom

In England, the principle of double jeopardy is well established and has its origins in 12th-century common and ecclesiastical law. The modern principle of double jeopardy in English law was set out by the Divisional Court in *Fofana v. Deputy Prosecutor Thubin, Tribunal de Grande Instance de Meaux, France*:

> *The authorities establish two circumstances in English law that offend the principle of double jeopardy:*
> *(1) Following an acquittal or conviction for an offence, which is the same in fact and law* – autrefois acquit *or* convict*; and*
> *(2) following a trial for any offence which was founded on 'the same or substantially the same facts', where the court would normally consider it right to stay the prosecution as an abuse of process and/or unless the prosecution can show 'special circumstances' why another trial should take place.*[36]

33 The protection is not absolute. A second trial is permitted in defined circumstances. In the United Kingdom, a prosecutor will seek a retrial if a jury has been unable to reach a verdict in the initial trial. A further trial in murder cases may also be permitted in circumstances where compelling new evidence comes to light.

34 U.S. Const. amend. V.

35 See generally Ernest H Schopler, Annotation, Supreme Court's Views of Fifth Amendment's Double Jeopardy Clause Pertinent to or Applied in Federal Criminal Cases, 50 L. Ed. 2d 830 (2012).

36 [2006] EWHC 744 (Admin), Judgment at para. 18.

The Divisional Court referred expressly to the United Kingdom's adoption of Article 54 of the Schengen Convention and its underlying rationale.[37] This is particularly important, as Article 54 states that a person (or company) whose case has been 'finally disposed of' by one Contracting Party may not be prosecuted by another for the 'same acts', provided that any penalty imposed has been enforced or is being enforced.[38]

Throughout the judgment, the Court stressed the need to look at the underlying acts behind each charge, rather than the label of the charge itself. In the event, the Court stayed the extradition proceedings on the basis that, although the extradition offence specified in the warrant was not based exactly, or solely, on the same facts as those charged in the UK indictment, there was such significant overlap between them as to require the proceedings to be stayed.[39]

In the case of *DePuy International Limited*, the SFO applied the double jeopardy principle and confirmed that it will likely arise where there is or has been an investigation into the defendant's conduct by another authority overseas and the essence of a criminal offence in England and Wales is the same offence for which the defendant already faces trial, or has been acquitted or convicted. DePuy was a UK subsidiary of Johnson & Johnson, a US company that self-reported to the DOJ and the SEC bribery of foreign officials by DePuy, as well as other offences that did not involve the company, under the FCPA. Johnson & Johnson agreed to a DPA with the DOJ covering the FCPA violations and a civil sanction with the SEC that encompassed criminal and civil fines amounting to US$70 million.

The DOJ informed the SFO of the criminal conduct and the SFO commenced an investigation into DePuy and Mr Dougall, the company's marketing manager. The SFO took the view that the DPA agreed by the parent company with the DOJ had the legal character of a formally concluded prosecution that punished the same conduct that had formed the basis of the SFO investigation. It determined that the rule against double jeopardy prevented any further criminal sanction being applied in the United Kingdom and instead pursued the company using a civil route to obtain the proceeds of crime. The civil sum obtained by the SFO took into account the global settlement in the United States, including the civil fines paid and recovered of £4.8 million.

Whether a DPA under the United Kingdom's regime would qualify for double jeopardy protection remains an open question. Although entry into a DPA does not constitute a criminal conviction, it does become the final disposal of specific intended criminal proceedings on its expiry and is almost certain to include the enforcement of a fine against the corporate subject. Furthermore, prosecution may follow in the event of a breach of the DPA.

The *DePuy* case developed further in July 2019 with proceedings being brought in Greece against three UK nationals, Michael Dormer, Johnson &

37 Id. at para. 14.

38 In the United Kingdom, the decision to leave the EU adds further uncertainty to the recognition of double jeopardy principle in its application to convictions in other Member States.

39 [2006] EWHC 744 (Admin) Judgment at para. 29.

Johnson's former company group chairman, Gary Fitzpatrick, former vice president for finance at DePuy, and John Coppack, DePuy's former company secretary, as well as a number of Greek nationals. The three UK nationals were convicted of fraud and money laundering offences and sentenced to seven years in prison. As at the date of publication, these sentences are under appeal.

In addition to the convictions, the court acquitted six defendants of the charges, including DePuy's former legal director, Irene Kyriakides, and its former vice president, Robert John Dougall. Dougall was acquitted of the charges on double jeopardy grounds having already been convicted of taking part in the same bribery scheme in the United Kingdom in 2010. Some of the evidence Greek prosecutors sought to rely on to build a case against Dougall had come from the SFO following Dougall's co-operation under a section 73 Serious Organised Crime and Police Act 2005 agreement. At the Greek trial, the SFO's associate general counsel, Raymond Emson, testified to say that the agency had not consented to the use of its evidence to prosecute Dougall in Greece and that its continued use could harm UK public interest.[40]

1.2.2 Double jeopardy in the United States

As noted above, the Fifth Amendment to the US Constitution contains a double jeopardy clause. Generally speaking, the double jeopardy clause prohibits the US federal government, or any individual state, from twice prosecuting someone for the same conduct if that person has already been acquitted or convicted (or after certain mistrials once a jury has been empanelled and 'jeopardy has attached').[41] It also prohibits courts from imposing multiple punishments for the same conduct, which may be covered in multiple charges in an indictment.[42] The double jeopardy clause of the Fifth Amendment – unlike its privilege against self-incrimination – applies to both individuals and corporations.[43]

The US Supreme Court, however, has long recognised a significant exception to the double jeopardy clause, known as the 'dual sovereignty' doctrine. Pursuant to this, double jeopardy does not prohibit the federal government from prosecuting a person previously convicted or acquitted by a state, or *vice versa*, or one state from prosecuting a person convicted or acquitted by another.[44] In other words, under this doctrine the US federal government can prosecute individuals and entities for the exact same conduct that they have previously been tried for in

40 https://globalinvestigationsreview.com/article/1195671/greece-convicts-three-uk-nationals-in-johnson-johnson-bribery-case#.Xa3IneLu1GM.mailto and https://globalinvestigationsreview.com/article/1195718/former-johnson-johnson-execs-to-appeal-against-greek-bribery-convictions#.Xa3JQi_97kI.mailto.

41 See *U.S. Const. amend. V; Martinez v. Illinois*, 134 S. Ct. 2070, 2074.

42 See *Breed v. Jones*, 421 U.S. 519, 528 (1975).

43 See *United States v. Martin Linen Supply Co.*, 430 U.S. 564 (1977) (applying double jeopardy to corporate defendants without discussing their status as corporations); *United States v. Sec. Nat'l Bank*, 546 F.2d 492, 494 (2d Cir. 1976).

44 *Gamble v. United States*, 139 S. Ct. 1960 (2019). See also, *United States v. Lanza*, 260 U.S. 377, 385 (1922).

one of the states, regardless of whether they were convicted or acquitted in that prior case.[45]

In 2019, the Supreme Court, in *Gamble v. United States*, once again reaffirmed the dual sovereignty doctrine in upholding successive prosecutions of an individual by the state of Alabama and then by the United States for the same essential conduct.[46] Although *Gamble* involved purely US domestic conduct, the Court highlighted that the dual sovereignty doctrine helped ensure the United States retained authority to prosecute extraterritorial conduct – regardless of a foreign prosecution – to vindicate US interests. In arriving at this conclusion, the Court observed:

> *There are other reasons not to offload all prosecutions for crimes involving Americans abroad. We may lack confidence in the competence or honesty of the other country's legal system. Less cynically, we may think that special protection for US nationals serves key national interests related to security, trade, commerce, or scholarship. Such interests might also give us a stake in punishing crimes committed by US nationals abroad – especially crimes that might do harm to our national security or foreign relations.*[47]

The Court's cynicism aside, this decision clearly underscores the prudence of pre-resolution engagement with US authorities for companies and individuals facing investigations in a foreign jurisdiction where US interests might be implicated.

Nevertheless, while the law clearly allows successive prosecutions in such instances, to blunt the potentially harsh impact of the dual sovereignty exception, the DOJ has adopted a policy that precludes the initiation of federal prosecution following a prior state (or federal) prosecution based on substantially the same facts. The Dual and Successive Prosecution Policy (the Petite Policy) seeks:

> *to vindicate substantial federal interests through appropriate federal prosecutions, to protect persons charged with criminal conduct from the burdens associated with multiple prosecutions and punishments for substantially the same act(s) or transaction(s), to promote efficient utilization of Department resources, and to promote coordination and cooperation between federal and state prosecutors.*[48]

---

45 Notably, the Supreme Court very recently declined to extend the dual sovereignty doctrine to successive prosecutions by Puerto Rico and the United States, concluding that the question of separate sovereignty requires an assessment of the source of the power to punish. *Puerto Rico v. Sanchez Valle*, 136 S. Ct. 1863 (2016). There, the Court held that successive prosecutions may be brought only where two prosecuting authorities derive their power to punish from independent sources; if those authorities draw their power from the same ultimate source, successive prosecutions are prohibited.

46 *Gamble*, 139 S. Ct. at 1964.

47 Id. at 1967 (emphasis in original).

48 U.S. Dep't of Justice, Justice Manual §9-2.031 (1999).

To overcome this policy, federal prosecutors must not only comply with the standards applicable for commencing any federal prosecution (i.e., that the defendant's conduct constitutes a federal offence and that the admissible evidence probably will be sufficient to obtain and sustain a conviction by an unbiased trier of fact), but they must also obtain the approval of the appropriate Assistant Attorney General and establish that (1) the matter involves a substantial federal interest; and (2) the prior prosecution left that federal interest 'demonstrably unvindicated'. It is the second of these two factors that provides the greatest protection against successive prosecutions, as, under this policy, the DOJ 'will presume that a prior prosecution, regardless of result, has vindicated the relevant federal interest'.[49] While this presumption can, of course, be overcome (and the policy lists the factors relevant to make such an assessment),[50] federal prosecutors traditionally reserve such challenges for those cases where it perceives the preceding result to have been manifestly unjust.

Notably, the Petite Policy does not expressly preclude the DOJ from bringing criminal charges based on the same conduct previously prosecuted by a foreign sovereign. Nevertheless, similar, if not identical, principles are at play whether the prior prosecution was brought by a state or federal government, or a foreign sovereign. Counsel endeavouring to persuade the DOJ to defer to the foreign result certainly should be prepared to demonstrate why a successive prosecution would contravene that policy. The DOJ will, of course, consider if US interests have been sufficiently redressed by the foreign prosecution.[51] And, in the cases of corporate criminal activity, it is likely that the DOJ will seek to exact a penalty based on the harm to its interests.

Still, if a prior prosecution by a foreign sovereign has resulted in adequate penalties proportionate to the conduct, the DOJ may well decline or defer the prosecution or, perhaps, offset any US fines or penalties by the amounts paid abroad, particularly in the corporate context. This is particularly likely in the wake of the DOJ's new policy, announced in May 2018 and since incorporated into the DOJ's Justice Manual, to discourage the 'piling on' of multiple penalties by the DOJ and foreign and domestic agencies when they are investigating the same corporate misconduct.[52] The policy articulates certain factors to be used when determining whether the imposition of multiple penalties would nevertheless serve the interest of justice, and therefore there is no certainty that prior prosecution by a foreign sovereign will result in no or lenient punishment by the United States.

The double jeopardy clause generally does not restrict the ability of the US government to pursue successive criminal and administrative remedies for the

49 Id.

50 Id.

51 See *Thompson v. United States*, 444 U.S. 248, 248 (1980) (noting that there is an exception to the Petite Policy where US prosecution would serve 'compelling interests of federal law enforcement').

52 US Dep't of Justice, Justice Manual §1-12.100; Deputy Att'y Gen. Rod Rosenstein, Remarks to the New York City Bar White Collar Crime Institute (9 May 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

same conduct.[53] Indeed, while it is more common for administrative investigations to run in parallel with DOJ investigations, double jeopardy is not offended when a criminal prosecution follows the imposition of an administrative sanction (or *vice versa*). As the Supreme Court held in *Hudson v. United States*, the double jeopardy clause does not apply to non-criminal penalties.[54] Though the Court in *Hudson* recognised that criminal charges following in the wake of stinging administrative penalties could potentially implicate double jeopardy concerns, a defendant mounting such a challenge must establish by the 'clearest proof' that the administrative penalty was so punitive as to render it criminal for double jeopardy purposes – a very high hurdle indeed.[55]

The application of double jeopardy in the EU and under the ECHR 1.2.3

Increased focus on combating overseas corruption following the signing of the Organisation for Economic Co-operation and Development's Convention on Combating Bribery of Foreign Public Officials in International Business Transactions has resulted in a rise in multiple prosecutions. A person or company engaging in overseas corruption faces the prospect of prosecution in any signatory country where he, she or the company may have sufficient involvement, either by citizenship or place of incorporation, or as a place where relevant acts took place.

The picture is evolving on both the supranational and national levels, and this is discussed below. The double jeopardy principle is set out in Article 54 of the 1985 Schengen Agreement.[56] On 29 May 2000, the United Kingdom adopted Article 54 of the Schengen Convention and so it presently forms part of the domestic law.[57] The rationale for the application of the principle across the European Union was made clear in *R v. Gozutok and Brugge*,[58] as permitting finality in criminal proceedings and also engendering mutual trust in national criminal justice systems by requiring that each Member State recognise the criminal laws in force in the others even when the outcome would be different if its own national law had been applied.

The Council Framework Decision 2009 on the prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (the EU Framework Decision)[59] sets out measures to prevent situations where the same person is subject to parallel criminal proceedings in different Member States in respect of the

53 See *Hudson v. United States*, 522 U.S. 93, 96 (1997).

54 Id. at 99.

55 See id.

56 Article 54: 'A person whose trial has been finally disposed of in one contracting party may not be prosecuted in another contracting party for the same acts provided that, if a penalty has been imposed, it has been enforced, is actually in the process of being enforced or can no longer be enforced under the laws of the sentencing contracting party.'

57 2000/365/EC: Council Decision of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis.

58 [2003] 2 CMLR 2.

59 2009/948/JHA.

same facts that might lead to the final disposal of those proceedings in two or more Member States.

The EU Framework Decision is constitutionally binding on the United Kingdom as a Member State and as such must be taken into account by the SFO in its decision whether to open a criminal investigation. The double jeopardy principle is not a bar to a criminal investigation, however, and the SFO has very wide discretion in deciding whether to carry out an investigation.[60]

1.2.4 European human rights jurisprudence

1.2.4.1 European Court of Human Rights (ECtHR)

Article 4 of Protocol 7 to the European Convention on Human Rights (ECHR) specifically recognises the double jeopardy principle.[61]

The importance of the principle was emphasised in the ECtHR's Chamber judgment in the case of *Grande Stevens and Others v. Italy*.[62] Here, the applicants received an administrative penalty from Consob, the Italian Companies and Stock Exchange Commission, in respect of providing false or misleading information concerning financial instruments. The penalty took the form of substantial fines and various banning orders. Subsequently, the applicants were committed for trial before the Turin District Court in respect of criminal allegations of market abuse arising out of the same facts.

The applicants argued before the ECtHR that the subsequent criminal proceedings were in breach of Article 4 as the applicants had already been subject to a penalty that was akin to a criminal penalty, even though it was imposed in an administrative context. The court accepted their argument and ruled that the administrative penalty should be considered a criminal penalty for the purposes of the ECHR and that Article 4 prevented the criminal proceedings from taking place on the grounds of double jeopardy.[63]

---

60 Section 1(3) of the Criminal Justice Act 1987: 'The Director may investigate any suspected offence which appears to him on reasonable grounds to involve serious or complex fraud.' See also *R (Corner House) v. Director of the SFO* [2008] EWHC 714 (Admin) at para. 51.

61 *Article 4 – Right not to be tried or punished twice*

1 No one shall be liable to be tried or punished again in criminal proceedings under the jurisdiction of the same State for an offence for which he has already been finally acquitted or convicted in accordance with the law and penal procedure of that State.

2 The provisions of the preceding paragraph shall not prevent the reopening of the case in accordance with the law and penal procedure of the State concerned, if there is evidence of new or newly discovered facts, or if there has been a fundamental defect in the previous proceedings, which could affect the outcome of the case.

3 No derogation from this Article shall be made under Article 15 of the Convention.

62 *Grande Stevens and Others v. Italy* (4 March 2014) Application Nos. 18640/10, 18647/10, 18668/10 and 18698/10.

63 In March 2015, France's Constitutional Court ruled that Airbus executives could not be prosecuted for insider trading because they had been cleared over similar administrative charges by France's Financial Markets Authority, the AMF. In reaching its decision, the Court gave considerable weight to the decision of the ECtHR in the *Grande Stevens* case.

The Court of Justice of the European Union (CJEU) 1.2.4.2

2018 saw three further cases arising in Italy where the principle of double jeopardy was considered, again in relation to administrative penalties imposed by Consob which were severe enough to be considered criminal in nature. All these cases were referred to the CJEU by Italy's Supreme Court of Cassation for a preliminary ruling considering Article 50 of the Charter of Fundamental Rights of the European Union and Article 4, Protocol 7 ECHR.

In the *Ricucci* matter,[64] the defendant had been fined €10.2 million by Consob, as well as being convicted in criminal proceedings resulting in a sentence of four years' imprisonment for alleged market manipulation. The Rome District Court subsequently pardoned Ricucci in a final judgment.

Ricucci challenged Consob's fine in Rome's Court of Appeal, which reduced it to €5 million in 2009. He then took his appeal to Italy's Supreme Court of Cassation, where he argued that his 2008 criminal conviction and subsequent pardon should negate any Consob proceedings. The Court of Appeal asked the CJEU whether the *ne bis in idem* principle in Article 50 gives individuals a direct right that can be applied to negate dual proceedings. The Court also asked the CJEU whether the *ne bis in idem* principle precludes Italy's law allowing administrative proceedings to be brought for market manipulation after a defendant has been finally convicted.

The CJEU held that dual proceedings can be pursued if they meet 'an objective of general interest' – in this case, to protect the European Union's financial interests. However, the national legislation must also ensure that proceedings and the severity of penalties are limited to 'what is strictly necessary' where dual proceedings are to be pursued. Italy's market manipulation law did not respect the principle of proportionality, and the CJEU ruled that, if a criminal penalty already punishes misconduct in an 'effective, proportionate and dissuasive manner', administrative proceedings of a criminal nature are gratuitous and so go beyond 'what is strictly necessary'.

In two other cases, *Di Puma* and *Zecca*,[65] appeals were made against Consob fines, with the defendants arguing that they should not face administrative charges for insider trading when a criminal court had found no misconduct. The appeals court asked the CJEU whether, in light of *ne bis in idem*, a court would violate an EU directive that requires Member States to provide 'effective, proportionate and dissuasive penalties' for insider trading if it did not bring administrative sanctions after a criminal court found no wrongdoing.

The CJEU determined in its preliminary ruling that not bringing administrative sanctions after a criminal court has found no misconduct is in accordance with EU law because of the principle of *res judicata*. It ruled that a defendant who

64 Case C-537/16: Judgment of the Court (Grand Chamber) of 20 March 2018 (request for a preliminary ruling from the Supreme Court of Cassation – Italy). See also https://globalinvestigationsreview.com/article/1168169/cjeu-italian-defendants-should-not-face-double-jeopardy.

65 Joined Cases C-596/16 and C-597/16, *Di Puma and Zecca*.

is cleared of a criminal charge should not be the subject of administrative proceedings for the same matter.

The CJEU has considered the application of the double jeopardy principle to the Schengen Agreement in the context of an individual under investigation in Poland and Germany for allegations of extortion.[66] In this case it upheld the German prosecutor's decision that the double jeopardy principle did not apply. The matter had not been finally disposed of as no detailed investigation had taken place.

On 15 November 2016, the CJEU rejected an appeal brought by two applicants who were penalised by the Norwegian Tax Authority for failing to pay tax in 2008 and then convicted of aggravated tax fraud in 2009 by the National Authority for Investigation and Prosecution of Economic Crime. The applicants claimed they were being prosecuted twice for the same misconduct in violation of double jeopardy rules. Rejecting the application, the court held that ECHR double jeopardy rules are not violated where the contracting party could satisfy the court that dual proceedings are sufficiently connected in time and space so as to represent a coherent whole, rather than two sets of proceedings.[67]

1.2.5 Double jeopardy in France

Recent developments in France continue to warrant a special mention as the issue of double jeopardy and its application has come before the courts on a number of occasions in recent years. The appellate courts have considered the extent to which domestic law will recognise convictions in the United States as a bar to prosecution, as well as the status of US DPAs in domestic proceedings. On 18 June 2015, a criminal court in Paris acquitted four French companies that were accused of paying bribes in connection with the United Nations' Oil-For-Food Programme on the grounds that they (or their corporate parents) had already signed DPAs with the DOJ. The rationale given was that it was inconsistent with French international obligations to prosecute the companies for a second time on what the Court found to be the same facts. The prosecutor's appeal against the acquittal was successful and in February 2016 a Paris court fined Total SA €750,000 for corrupting foreign officials.

Separate criminal proceedings were successfully pursued in France against Total for corruption of a foreign public agent (a senior energy official in Iran) resulting in a €500,000 fine being imposed in December 2018. The prosecution unsuccessfully sought confiscation €250,000 it had argued were the proceeds of the corruption. In relation to the same matters, Total entered into a US$245.2 million, three-year DPA with the DOJ and disgorged US$153 million in an SEC cease-and-desist order. The DPA expired in November 2016.

On 26 February 2018, the Court of Cassation in Paris upheld a decision to fine Swiss energy company Vitol €300,000 for making corrupt payments to the

66 Case C-486/14, *Kossowski*, 29 June 2016.

67 *Case of A and B v. Norway* (Applications nos. 24130/11 and 29758/11), 15 November 2016, lovdata.no/static/EMDN/emd-2011-024130.pdf.

Iraq government as part of the United Nations Oil-For-Food programme.[68] The Court rejected Vitol's argument that it was protected from criminal proceedings in France because it had already been punished in the United States. The Court found that double jeopardy did not apply because the company had pleaded guilty to a different charge in US proceedings[69] and stated that France must maintain its right to punish companies that break French law. In its ruling, the Court of Cassation considered double jeopardy protections enshrined in both France's Penal Code and the Charter of Fundamental Rights of the European Union. It concluded that both those protections fail to immunise a company from being prosecuted twice if part of the offence occurred within France and if the misconduct is prosecuted by a country that is not bound by French or EU law, such as the United States.[70] This significantly weakens the double jeopardy defence, in circumstances where some of the misconduct occurred in France.

These cases demonstrate the potential unfairness to a corporate that has effectively admitted the offence in another jurisdiction to obtain a DPA and then finds those admissions being used against it in a jurisdiction that does not recognise the DPA under the double jeopardy doctrine.

Conclusion 1.2.6

At first sight, the doctrine of double jeopardy appears to be a substantial protection against repeated prosecution in respect of the same conduct. However, although the doctrine may in some circumstances protect against a similar prosecution within the state, or member group such as the European Union, it may well fail to protect against a prosecution brought by a separate state. France's decision not to apply the principle in circumstances where part of the offence occurred within its sovereign territory is a significant restriction on its scope.

As many countries do not recognise a foreign conviction for the purposes of double jeopardy, it is not possible to reassure a corporate client that a criminal settlement in one jurisdiction will qualify as a settlement in others as well. Further, entering into a DPA in one jurisdiction may risk damaging the client's interests in another if the DPA is not recognised as a bar to prosecution, but the admissions it made to secure the DPA are admissible against it in other jurisdictions.

The picture is uncertain and many questions remain unanswered. These include:

- Should there be international recognition of criminal convictions for the purposes of double jeopardy, to encourage global settlements?

68 The fine was in addition to a US$17.5 million sanction Vitol received in the United States in 2007 as part of a plea agreement entered to resolve identical allegations.

69 The company pleaded guilty to a single count of grand larceny in the New York State Supreme Court and paid a US$17.5 million fine, US$4.5 million of which was donated to the state of New York. Vitol admitted in the US plea deal that corrupt payments were made through its employees in France. In total, the company said it paid US$13 million to Iraqi officials between 2001 and 2002 hidden in oil contracts awarded to the company as part of the Oil-For-Food programme.

70 Note that as France is a civil law jurisdiction, lower courts are not strictly bound to follow the Court of Cassation's decision.

- Should DPAs be given the status of a criminal conviction for the purposes of double jeopardy?
- Should regulatory sanctions qualify for the purposes of double jeopardy?

Until these issues are resolved, a corporate client will only be able to place very limited reliance on the double jeopardy principle as a bar to further prosecution in respect of the same conduct. At present, the only safe course will be to seek to negotiate a global settlement with all the states most likely to take an interest in the conduct, before admitting guilt in any state. Whether this is practicable will vary from case to case.

In relation to individuals, an issue of note was recently referred to the CJEU stemming from a dispute between Hungary and Croatia in the case of *AY*.[71] The Croatian court had sought a preliminary ruling on whether the double jeopardy principle under EU law means Member States may refuse to enforce European arrest warrant (EAW) requests in cases where its investigations treated individuals as witnesses and not suspects. Specifically, Croatia asked whether Hungary could refuse to enforce two EAW requests it issued for an individual, named only as AY, to prevent damage to reputation, after AY was treated as a witness rather than a suspect in an investigation conducted by the Hungarian prosecutor's office. In its judgment of July 2018, the CJEU stated that execution of an EAW cannot be refused on the ground that a prosecutor had closed a criminal investigation where, during that investigation, the requested person was interviewed as a witness only. The Court stated that the judicial authorities of the Member States must adopt a decision on any EAW communicated to them.

71 Judgment in Case C-268/17 *AY (Arrest warrant – witness)*. The Court analysed whether any of the grounds for optional non-execution provided for in Article 4(3) of the framework decision applied in the *AY* case and concluded they did not. Those grounds relate to (1) the decision of the executing judicial authority not to prosecute for the offence on which the European arrest warrant is based, (2) the fact that, in the executing Member State, the judicial authorities have decided to halt proceedings in respect of the offence on which the warrant is based, and (3) the fact that a final judgment has been passed on the requested person in a Member State, in respect of the same acts, which prevents further proceedings. The Court determined the first and third grounds were irrelevant in the case. The Court concluded that an interpretation according to which the execution of a European arrest warrant could be refused where that warrant concerns the same acts as those that have already been the subject of a previous decision, without the identity of the person against whom criminal proceedings are brought being considered relevant, would be manifestly too broad and would entail a risk that the obligation to execute the warrant could be circumvented. As that ground for non-execution constitutes an exception, it must be interpreted strictly and in the light of the need to promote the prevention of crime. The investigation by the Hungarian authorities was conducted, not against AY, but against an unknown person, and the decision that closed that investigation was not taken in respect of AY. The Court concludes from this that the second ground for non-execution does not apply either. See also https://globalinvestigationsreview.com/article/1166589/croatian-case-to-clarify-eaw-double-jeopardy-rules.

The stages of an investigation 1.3

Issues that at first glance may appear to be isolated or technical can quickly spread across borders and escalate into multifaceted threats to businesses, reputations and careers. Even within jurisdictions, different enforcement authorities operate within their own, often complex, legal and technical frameworks. Any investigation, whether an internal fact-finding inquiry aimed at establishing the size and nature of a problem or one commenced by an enforcement authority, is inevitably a dynamic process. There can be no 'one-size-fits-all' approach and the scope of an investigation can change significantly as it progresses.

Nonetheless, it is possible to identify three broad, and often overlapping, phases to an investigation, namely the commencement, information-gathering and disposal phases. Particular challenges arise, and sometimes recur, at each of these.

Conducting and handling investigations, limiting the damage they cause and bringing them to as swift and efficient a conclusion as possible is an art rather than a science. It requires advisers to anticipate, balance and respond to a wide variety of challenges, and to appreciate the potential ramifications of every interaction with a diverse cast of characters.

Commencement 1.3.1

When deciding whether or how to commence an investigation, or how best to respond to one already commenced by an enforcement authority, it is axiomatic that the very first task to be carried out must be to establish as precisely as possible the size and shape of the problem. Which corporate entities and individuals are regarded as subjects of the investigation? Which offences are they thought to have committed, and which regulatory provisions might they have infringed? Are any other local or foreign agencies investigating (or likely to investigate) this misconduct?

In some cases (typically those involving alleged breaches of regulatory requirements), the answers will be self-evident from notices from authorities confirming the commencement of an investigation or the appointment of investigators, and there may be opportunities to seek to establish more detail through scoping discussions. However, in other cases (typically those involving alleged criminal misconduct), the investigators will not necessarily provide details or opportunities for discussion. In some cases, the first indication an individual or entity receives of an investigation by an enforcement authority will be a requirement to attend an interview or provide documents, or, worse still, a knock at the door from investigating officers. In all cases – whether or not enforcement authorities are already aware of alleged misconduct – steps must be taken immediately upon discovery of the alleged misconduct to preserve and to avoid the destruction or deletion (inadvertent or otherwise) of documents that are, or could become, relevant. In large multinational organisations, identifying the custodians of these documents, drafting and disseminating appropriately inclusive document-retention notices, gathering the material and suspending automatic deletion policies is a substantial undertaking in itself.

Where authorities are not already aware of apparent misconduct, considering whether, when and how to disclose matters to them will be an immediate priority. In some cases, specific regulatory obligations will require disclosures. In others, it may be appropriate to voluntarily report matters to maximise the prospects of a consensual resolution on favourable terms. Both types of disclosures require careful handling. Consideration must be given to potential consequences, both for those individuals or corporates already implicated in alleged misconduct, and for those that may become so. Where information is disclosed voluntarily, wider considerations about whether co-operation will be appropriate and would be likely to encourage the relevant enforcement authority to curtail its investigation (and on which terms) should be borne in mind. Identifying the potential risks and benefits will typically involve assessing the enforcement policy and posture of each agency involved (and often of individual investigators) and its ability and propensity to pass information to other investigating or prosecuting authorities (both within and between jurisdictions).

These assessments will inform the answers to a number of practical questions:

- Should an initial notification be made before a full internal investigation has been undertaken?
- What should be disclosed at the end of the internal investigation and to whom?
- Should information be disclosed to the authorities orally rather than in writing?
- Will investigators regard anything less than unfettered access to witnesses' first accounts and other underlying documents as true co-operation enabling them to contemplate a negotiated outcome?
- Is it feasible to maintain claims to legal professional privilege or challenge investigators' actions or demands while still seeking to claim that the subjects of the investigation are co-operating?

Some of these questions have been addressed in the SFO's Corporate Co-operation Guidance, published in August 2019.[72] This provides greater clarity on the circumstances in which the SFO will be prepared to commence discussions with a view to potentially concluding investigations by way of DPAs.

Choices made at this stage about how much information and control to relinquish over the investigative process and the robustness of the line to be taken with investigators in relation to issues such as privilege can be crucial in setting the tone for the rest of the investigation, and any proceedings that flow from it. It is critical for companies, when deciding which stance to take at the commencement stage, to anticipate what enforcement authorities and courts may require at later stages and what the collateral effect of decisions about how much information to provide and how proactively to assist those authorities may be. The DPA agreed between the SFO and Sarclad illustrates this point. Following the conclusion of the DPA, former senior executives being prosecuted by the SFO sought to compel the SFO to obtain and disclose to them copies of notes of interviews relevant to

72 https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

the SFO's decision to enter into a DPA with the company.[73] The notes had not been previously provided to the SFO during DPA negotiations as Sarclad declined to waive privilege and the SFO agreed to proceed on the basis of summaries of the interviews prepared on the basis of 'oral proffers' delivered by Sarclad's lawyers. Although the High Court, hearing the challenge brought by the former senior executives being prosecuted (and who were subsequently acquitted in July 2019) declined to order the SFO to obtain and disclose the additional documents, it deprecated the approach taken by the SFO. As a consequence, as is confirmed in its Corporate Co-operation Guidance, the SFO is likely to take a more stringent approach when deciding which documents it requires during DPA negotiations.

Before the publication of the third edition of this text, the Court of Appeal allowed ENRC's appeal against the first-instance decision, upholding its claim to litigation privilege over the disputed documents, including notes of witness interviews.[74] Under the leadership of the Director of the SFO, Lisa Osofsky, the SFO decided not to appeal that decision. Given the importance of privilege in the context of global investigations, the decision was welcomed by lawyers across the globe – the Court of Appeal's judgment aligned the law more closely with the law of privilege in the United States and its clear articulation of the applicability of litigation privilege in the context of a criminal investigation is likely to mean that the SFO will be less aggressive in making assertions that privilege claims by companies over documents created during the course of internal investigations are ill-founded than it was before the ruling. However, it is unlikely that the SFO will be any less willing to request waivers of privilege, particularly since the Court of Appeal judgment was clear that its decision should not 'impact adversely' on the deferred prosecution regime in the United Kingdom, and emphasising the relevance of waiver to an assessment of a company's co-operation in reaching resolutions.[75] The SFO's Corporate Co-operation Guidance addresses this point but does not provide a definitive answer. It acknowledges (as is evident from the DPAs concluded to date) that declining to waive privilege is not necessarily fatal to a settlement subsequently being agreed and simply states that a company declining to waive privilege does not attain the corresponding benefit set out in the DPA Code of Practice, but will not be penalised by the SFO. In practice, this superficially neutral stance is likely to translate into significantly more difficult discussions, both with the SFO about whether it is appropriate to commence DPA negotiations, and in due course with the SFO and the court about whether any proposed DPA should be concluded and approved. Decisions as to the approach taken by a company to privilege, regardless of whether privilege can properly be asserted or

73 *R (on the application of AL) v Serious Fraud Office* [2018] EWHC 856.

74 *SFO v. ENRC* [2018] EWCA Civ 2006.

75 See *SFO v. ENRC* [2018] EWCA Civ 2006 at paras. 115–117, in particular: 'In any event, to determine whether a DPA is in the interests of justice, and whether the terms of the particular DPA are fair, reasonable and proportionate, the court must examine the company's conduct and the extent to which it cooperated with the SFO. Such an examination will consider whether the company was willing to waive any privilege attaching to documents produced during internal investigations, so that it could share those documents with the SFO . . .'

not, will continue to be crucial decisions that set the tone and, possibly, direction of an investigation and any proceedings flowing from it.

In cases involving allegations made by or against directors or employees, early determinations need to be made as to whether any specific whistleblower protection legislation or rules have been engaged and whether action should be taken to suspend or dismiss those individuals, or at least limit their involvement in decision-making in relation to investigations.

1.3.2 Information gathering

Once the scope of an investigation has been determined, the process of gathering and analysing relevant information, whether in documentary or electronic form or in the form of witnesses' accounts, commences. Since the advent of the European investigation order (introduced in England and Wales in 2017), the process of gathering information across borders has been a much simpler and quicker process for enforcement authorities in Europe.[76] In October 2019, the SFO's (and other agencies') powers were further extended as new legislation came into force enabling them to apply to the court to secure access to electronic data held by communications services providers overseas (provided certain international co-operation agreements are in place in the jurisdiction concerned).[77]

In substantial cross-border investigations, the task of collating relevant material, ascertaining whether it is responsive to requirements to produce documents or provide information (or whether it should otherwise be produced to demonstrate a co-operative stance), and filtering it to remove material exempt from disclosure is time- and resource-intensive. It often requires specialist technical input and expertise. Information should not be treated as a readily portable commodity, and careful consideration should be given to applicable data protection and other confidentiality constraints before information is transferred between jurisdictions during internal investigations or produced to investigating authorities.[78]

Witness interviews during internal investigations raise no fewer questions. When should interviews take place? Who should be present? What material and questions is it appropriate to put to them during such interviews? Should they be

76 See Criminal Justice (European Investigation Order) Regulations 2017.

77 See Crime (Overseas Production Orders) Act 2019.

78 Recent developments in the United Kingdom and United States are relevant. In the United Kingdom, a decision by the Administrative Court in September 2018, *R (on the Application of KBR Inc) v. The Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), extended section 2 notices, served in the United Kingdom, extraterritorially to foreign companies in respect of documents held outside the jurisdiction when there is a sufficient connection between the company and the jurisdiction. KBR received permission to appeal in April 2019 (https://www.supremecourt.uk/docs/permission-to-appeal-2019-04.pdf). In the United States, following the successful appeal by Microsoft of orders holding it in contempt for failure to comply with a warrant requiring it to produce the contents of a customer's email account stored on a server outside the United States, Congress enacted on 23 March 2018 the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), providing expressly for extraterritorial application and thereafter the United States obtained a fresh warrant against Microsoft.

represented (and, if so, at whose expense)? Taking a wider view across all jurisdictions in which action could be taken, and from the individual's perspective, is it in the interests of subjects of the investigation to provide information voluntarily, or should they insist on being compelled to do so?

Of course, where investigations by the authorities have already begun, investigating authorities will be keen to interview individuals who are suspects. Depending on the nature of the investigation and the allegations against them, it may be open to individuals to remain silent in response to questions (although this course of action may limit their options in any proceedings flowing from the investigation). Conversely, it may serve such individuals' interests to proactively volunteer information to secure more lenient treatment by authorities, or ultimately the courts.

Disposal 1.3.3

As the information gathering progresses, and evidence is assimilated and understood, a decision will need to be reached as to whether this may be resolved through negotiation, or whether the individual or company disputes the allegations entirely or is unprepared to reach any resolution or enter into any settlement that requires admissions of misconduct.

Where settlement is an option, from economic, commercial and reputational standpoints, settling with as many investigating authorities as quickly and on the most favourable terms possible is likely to be preferable. Particularly in regulatory enforcement investigations involving companies, it is often clear from the commencement phase that this will be the most likely outcome, and dialogue throughout the investigation will have to be directed towards this outcome.

It should not be assumed that the process leading to a negotiated disposal is a smooth or simple one. Even in cases involving only one enforcement authority, the legislation and rules governing settlement and the calculation of penalties are complex. Although the discounts available for early settlement are potentially significant, the processes leading to them can involve successive rounds of proposals, counterproposals, representations and negotiations. In criminal investigations, in jurisdictions where it is possible to achieve negotiated outcomes as an alternative to prosecution, although the degree of scrutiny varies depending on which jurisdiction is concerned, such settlements will also be examined by a judge.

Complexity is multiplied where multiple authorities or jurisdictions are involved, or where it is possible that a finding, even if it does not involve any admission of liability, may fuel subsequent litigation from third parties such as erstwhile customers, employees or shareholders.

Although major investigations are unlikely to have progressed to the disposal stage without attracting at least some publicity, it is at this stage that press and political interest will peak. Enforcement authorities usually must make the outcomes of investigations public (and indeed corporate entities themselves may be obliged to do so if their securities are listed).

Other difficult questions arise with negotiated disposals. What will be the size of the fines, if any? For individuals, is there the prospect of imprisonment or

other career-threatening penalties? Will it be possible to settle with all interested investigating authorities? For the corporate to bring matters to a close, will it be necessary to assist authorities in their pursuit of individuals? Will the disposal of the investigations mark the end of the matter, or simply the start of a new phase of litigation or the commencement of a long process of reporting to a monitor and heightened levels of regulatory scrutiny or supervision? What can be said publicly by the subjects of the investigations?

With these themes in mind, we turn now to a detailed consideration of each stage in the chapters that follow.

2

The Evolution of Risk Management in Global Investigations

William H Devaney and Joanna Ludlam[1]

Sources and triggers for investigations 2.1

Corporates have traditionally approached investigations reactively, after the event, as an issue for legal functions and law firms that is largely concerned with suspicions of criminal activity or other misconduct. Such investigations were predominantly an exercise in detection, appropriate reporting and remediation. With the evolution of compliance departments and advances in forensic fact-gathering and analysis, investigations are increasingly regarded as key elements of a sound control environment and generally considered to support a company's commercial agenda.[2]

Now, problems can be discovered through a variety of novel and increasingly proactive ways, and can arise from both internal and external sources.

From an internal perspective, problems can come to the fore during transactional due diligence, or in the course of routine compliance activity, such as conformance reviews, financial and other audits, or corporate surveillance activity. Problems may also be signalled by industry-wide regulatory enforcement, or in a discrete area concerning allegations against an employee that indicates broader risk. Corporate awareness of risk may also be triggered through traditional or social media, political pressure, customer complaints, allegations arising in civil litigation, statements made in evidence in regulatory or criminal proceedings, and disclosures by competitors and whistleblowers. Corporations are now also

1 William H Devaney and Joanna Ludlam are partners at Baker McKenzie LLP.

2 US Department of Justice (DOJ), Evaluation of Corporate Compliance Programs, April 2019, Sections I.A – D, II.B and III.A (noting the importance of risk assessments, training, communications, confidential reporting structures and investigative processes to inform an effective corporate compliance programme and identifying, inter alia, root causes and systems vulnerabilities). See https://www.justice.gov/criminal-fraud/page/file/937501/download.

encouraged to use artificial intelligence to sift through their own data to uncover indicia of potential wrongdoing.

Problems may also be first identified through the direct intervention of a government agency, which may have learned of the issue on its own, through a third party or another agency. The provision of information between law enforcement and regulatory authorities (whether through informal communication protocols, established statutory gateways or recognition of competing jurisdictions) is a rapidly growing area, domestically and internationally.

Given the myriad of potential avenues for a crisis to develop, corporate counsel must always be on the lookout for the seeds of problems and be prepared to take appropriate steps to prevent the matter from taking root and distracting the company from its core business. Moreover, if a serious problem is identified and cannot be easily contained, an effective response may require a significant level of communication with, and ongoing reporting obligations to, multiple entities, including the company's board and senior management; its legal, compliance, risk and audit functions; external auditors; prosecutors, regulators or other government agencies; litigation counterparties; investors; customers; commercial partners; competitors; trade bodies; and other interest groups. In many cases, the simple gathering of facts and their analysis can be one of the least complex elements of the undertaking. Far more complex is the juggling of competing, often cross-border, legal principles, interests and priorities that these ongoing communication and reporting processes require. These are considered further below, together with some of the complicated legal issues they present.

2.2 Responding to internal events

Not all internal issues raised will require investigation. Take, for example, the self-described whistleblower who writes to senior management to raise points already conclusively determined in a disciplinary hearing, in relation to which there are no wider considerations or further rights to appeal. Where facts are not in issue, the person has exhausted his or her legal remedies and does not bring forward new *bona fides* issues, a corporation should not be deterred from operating efficiently and need not reinvestigate the underlying facts. Those concerns that do merit fresh investigation will not necessarily arise only in the context of criminal allegations or regulatory misconduct; some will emerge during transactional due diligence or in the control environment. There may also be instances where even if the allegation is true, it does not amount to a violation of law or company policy.

2.2.1 Compliance operations and transactional due diligence

A critical aspect of any effective transactional due diligence – whether an acquisition, a joint venture or simply a one-off transaction – must necessarily be to identify risks lurking beneath the surface of a target business or transaction counterparty. In particular, attention to areas that can give rise to successor liability should be of paramount concern to the risk-assessment team on any due diligence. In the anti-money laundering arena, in relation to the United Kingdom,

compliance with the Proceeds of Crime Act 2002[3] is only as effective as the quality of the due diligence, ongoing monitoring and surveillance techniques employed by the company. Similar considerations apply to compliance with international sanctions, where certainty as to the true source of remitted funds, the purpose of the payment and the identities of the payor and payee are central. 'Adequate procedures' required under the UK Bribery Act 2010 will include the ability to assess counterparty risk to avoid participation in a corrupt transaction. In the United Kingdom, there has been a concerted move to replicate the corporate 'failure to prevent' offence in section 7 of the Bribery Act 2010 in other arenas, increasing the focus on the adequacy of prevention measures within corporations. Part 3 (sections 44 to 52) of the Criminal Finances Act 2017 created the offence of failing to prevent the facilitation of tax evasion, with the corresponding defence of 'reasonable prevention procedures'. In January 2017, the UK government consulted on the introduction of a general corporate offence of failing to prevent economic crime going beyond bribery and tax evasion, whereby companies would be liable for fraud by their employees or contractors in the absence of proof of adequate procedures to prevent the conduct.

The concerns in the United States are similar. The Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) have stated in their Resource Guide to the Foreign Corrupt Practices Act (FCPA) that they will be less likely to prosecute an acquirer that conducts effective pre-transactional due diligence, remediates, folds the acquired entity into its compliance programme and voluntarily discloses the conduct.[4] In 2018, US Deputy Assistant Attorney General Matthew Miner stated that the DOJ's revised FCPA Corporate Enforcement Policy (providing for a presumption of a declination of prosecution with disgorgement of ill-gotten gains, assuming no aggravating circumstances, for companies that voluntarily disclose, fully co-operate and fully remediate) would apply to acquirers in a merger or acquisition.[5] In March 2019, the DOJ formally codified this policy.[6] Further, while declinations under the FCPA Corporate Enforcement Policy are usually public and come with a statement of facts, Mr Miner recently said, in remarks he delivered at the American Bar Association's Third Global White Collar Crime Institute Conference, that 'there may be instances where a company self-discloses and [the DOJ] decide[s] a public declination is neither

3 Those necessary to enable a person or organisation to comply with reporting duties under §§ 330 to 332 and to avoid commission of separate money laundering offences under §§ 327 to 329 of the Proceeds of Crime Act.

4 A Resource Guide to the US Foreign Corrupt Practices Act (2012), 28 (discussing pre-transactional due diligence). See also US Department of Justice, Opinion Release 14-02 and Opinion Release 08-02.

5 See Matthew Miner, US Deputy Assistant Attorney General, Keynote Address at the American Conference Institute, 9th Global Forum on Anti-Corruption Compliance in High Risk Markets (25 July 2018).

6 See US Department of Justice, Justice Manual (JM) § 9-47.120 – FCPA Corporate Enforcement Policy, at 4 (M&A Due Diligence and Remediation).

necessary nor warranted'.[7] He noted that 'if a company self-discloses misconduct that was discovered in the context of a merger or acquisition, and [prosecutors] determine that the conduct and financial impact was *de minimis*, [the DOJ] may be open to a company's request that [the DOJ not] disclose the declination'.[8] Without delving into the pros and cons of voluntary disclosure, US law enforcement and regulatory agencies generally treat acquirers similarly even when the disclosure does not relate to potential FCPA violations, but to other issues such as money laundering and trade sanctions.[9]

See Chapters 3 and 4 on self-reporting to authorities

Given these expectations in the United Kingdom, United States and elsewhere, a party offering to warrant that it has not engaged in corrupt practices or other criminal activity will not provide adequate comfort without objective assessment of the risk profile, which is, itself, an exercise in investigation and analysis. For example, in the case of the three primary areas of financial crime risk (money laundering, sanctions, bribery and corruption), further enquiry may be required to investigate and assess the risk presented by politically exposed persons (PEPs), transactions involving higher-risk jurisdictions or business practices, complex transactional structures characterised by opacity as to source of funds and ultimate beneficiaries.

In each case it is not only the primary due diligence activities that require investigative skills, but also the response to the information delivered by standard or enhanced due diligence that may itself stimulate wider investigation. Concerns in open-source materials (such as reports from internet research and reports by Amnesty International and Transparency International's Corruption Perception Index), and information already held on file, in bespoke due diligence reports by third-party vendors and in responses from counterparties to questionnaires and pre-contractual enquiries (which are particularly prevalent in public sector contract due diligence) may all trigger separate lines of enquiry. Red flags such as opaque ownership structures, prior enforcement actions against the counterparty, engagement in high-risk geographies or the presence of PEPs in the ownership or control structure can all raise the risk profile of a person, entity or proposed transaction, putting the company on notice that further investigation is required.

Ironically, for companies straining to deliver strong due diligence, flagging issues of concern in clear, contemporaneous records at the primary due diligence stage may pose a significant danger. That record may create disclosable evidence of a company's state of knowledge and awareness, or the fact it was on notice, at a material time, and in the absence of an adequate investigative response, this record

7 Matthew Miner, US Deputy Assistant Attorney General, Remarks at The American Bar Association's Criminal Justice Section 3rd Global White Collar Crime Institute Conference held in Prague, Czech Republic (27 June 2019).

8 Id.

9 See John Cronan, Acting Assistant Attorney General, US Department of Justice Criminal Division, Presentation at the American Bar Association, White Collar Conference (1 March 2018) (conveying DOJ's intention to 'reward self-disclosure, full cooperation, [and] timely and appropriate remediation' by declining to bring cases against companies investigated for criminal violations other than under the FCPA).

itself may assist in incriminating the company[10] despite the positive steps taken to identify the issue in the first instance.

As such, it is the initial response that separates the strong organisation from the weak and moves compliance culture from a tick-box habit to best-in-class governance and control. The tools available to the acquiring company to assess possible exposure beyond the initial indicative information are a blend of the traditional and the innovative. The review of source documents and interviewing of witnesses are standard investigative steps that will remain highly relevant in these circumstances. So too will access to open-source information including historical media content analysis, materials held by ratings agencies and analyses based on public records, a company's data, disclosures and third-party commentary, social media, a company's public statements and reports, and bespoke assessments. Reports from third-party investigators (which can range from analysis of public records and open-source material to more detailed data searches, including 'dark web' internet content review) may also be available.

Additionally, internal and external audit reports may flag control weaknesses and identify intended remediation plans. These will not constitute privileged documents, although they may be subject to significant confidentiality controls. Action logs should be traced to ensure that audit recommendations were implemented and can be used as evidence of such. Similarly, analysis of compliance remediation and restructuring plans, conformance reviews of compliance systems and controls, published results of thematic reviews by regulators and other third parties, evaluation of whistleblower logs or statements made by company executives in the public domain (e.g., records of evidence adduced at UK parliamentary select committee or US congressional committee hearings) may also corroborate or appease initial concerns, or may serve to trigger further investigation into wider issues.

Some financial institutions go beyond this level of investigative activity and maintain an intelligence-based client evaluation process, aimed at building customer profiles in anticipation of commercial decisions and regulatory obligations. This is not for the use of investigators in the detection of misconduct but is research and analysis to provide the bank with the broadest range of commercial information about a client, customer or counterparty, from identification and verification through to commercial development strategy and market profile, to enhance the bank's strategic decision-making in a highly regulated environment. While these processes are driven by commercial objectives, the underlying activity necessary to inform the bank as to the risk profile is no different to the skills applied during a regulatory enforcement investigation or in anticipation of criminal prosecution, and this is why, within banks, there is a gradual migration of employees from 'investigations and enforcement' functions within legal and compliance to 'financial intelligence' units within business teams or as separate

10 For example, as evidence relevant to the offence in the United Kingdom of failing to prevent bribery under section 7 of the Bribery Act 2010 or in support of a regulatory enforcement for a suspected systems and controls breach under Principle 3 of the Financial Conduct Authority's (FCA) Principles for Businesses.

risk or compliance teams. These units do not, however, operate as legal advisers and therefore do not benefit from the same protections afforded to legal advisory staff, such as the attorney–client privilege and work-product protections (considered further below).

2.2.2 Policy guidance, opinion procedures and dialogue with public authorities

More formal, alternative third-party sources can provide a higher degree of comfort, subject to the availability of information and the legal and practical constraints as to its use. Use of these sources may be more appropriate where a company has identified a problem while undergoing due diligence. Nevertheless, practitioners should approach these resources with caution.

In the United States, for example, the DOJ may, on submission in writing by a relevant party, provide valuable guidance through the FCPA opinion procedure.[11] Similar to SEC no-action letters,[12] opinion procedures enable a corporation to obtain an opinion from the DOJ as to whether certain specified, prospective – not hypothetical – conduct does not violate the FCPA. The principles require disclosure of the entire intended transaction. An executed contract is not a prerequisite and in most cases the opinion would be sought prior to a requesting party's entering a contract. The DOJ's opinion will typically set forth a number of remedial or proactive steps, or both, that the company must take to receive protection from enforcement.[13] For example, in Opinion Release 08-02, a US company sought comfort from prosecution surrounding its proposed purchase of a UK company in the oil and gas sector. The UK company had a large number of government customers. The acquirer informed the DOJ that it had inadequate time and access to information to perform sufficient anti-corruption due diligence on the target. It further informed the DOJ that it could not disclose whether it had identified any possibly illicit payments owing to the confidentiality agreement it signed to receive access to information from the target. In its opinion, the DOJ said it would not initiate an enforcement action, so long as the acquirer disclosed any corruption concerns upon acquisition, conducted rapid and deep diligence (outlined in the opinion) once it owned the target, disclosed any potential violations it uncovered, and quickly folded the target into its compliance programme. In a 2018 keynote address at the Ninth Global Forum on Anti-Corruption Compliance in High Risk Markets, US Deputy Assistant Attorney General Miner

11 These can provide a high degree of comfort to corporations. See, for example, US Department of Justice Foreign Corrupt Practices Act Opinion Procedure Release 14-02 on successor liability principles, which assesses how the DOJ would approach the question of whether it would pursue wrongful pre-acquisition conduct by the target company where the target was not within the reach of the FCPA at the time of the alleged misconduct.

12 Securities and Exchange Commission (SEC) no-action letters allow individuals or entities unsure of the legality of a product, service or action to request a letter from the SEC discussing the facts, applicable laws and rules, and providing a conclusion about whether SEC staff would recommend an enforcement action. See https://www.sec.gov/.

13 For Opinion Procedure Releases, see https://www.justice.gov/criminal-fraud/opinion-procedure-releases.

encouraged the use of the opinion procedure process, noting that it is under-utilised, and stating that in terms of response times, the DOJ 'can, to a degree, expedite [its] analysis based on timing needs'. As Mr Miner outlined, the DOJ will respond within 30 to 45 days of receiving all necessary information.[14]

As demonstrated by the few opinions issued each year, practitioners are often wary of this process, and will likely remain so, despite Mr Miner's encouragement. First, if the DOJ says no, the company is left without any flexibility to make its own risk-based decision. It must comply. Additionally, as Opinion Release 08-02 demonstrates, the DOJ will often impose conditions and requirements in its opinion that must be adhered to meticulously. Further, seeking an opinion may risk tipping off the government about a larger problem. Opinion procedures are also a limited tool, as they apply only to anti-corruption concerns.

The United Kingdom does not have a process similar to the DOJ opinion procedure. There remains no formal basis on which to approach the Serious Fraud Office (SFO) for guidance as to whether a party's conduct infringes the Bribery Act 2010, for example. This evaluation is left to the reporting party, with the more binary decision as to whether or not to make an early self-report to the SFO in relation to which co-operation credit is sought. The SFO will publish operational guidance and Codes of Practice from time to time (e.g., on issues of treatment of evidence, witnesses and legal representation at interviews, deferred prosecution agreements (DPAs), corporate self-reporting and, most recently, corporate co-operation)[15] and, like the DOJ and SEC's Resource Guide to the FCPA, also publishes its related prosecution policies and protocols (such as the Bribery Act Joint Prosecution Guidance of The Director of the Serious Fraud Office and The Director of Public Prosecutions, Guidance on Corporate Prosecutions, etc.).[16] These are not, however, consultative processes aimed at clarifying the SFO's approach to legal interpretation or jurisdictional issues (as in the case of the DOJ opinion procedure or SEC no-action letters). The SFO has made clear on a number of occasions that its role is not that of 'regulator, an educator, an advisor, a confessor, or an apologist'[17] but of investigator and specialist prosecutor. It remains to be seen whether, under SFO Director Lisa Osofsky's leadership, which commenced in August 2018, the SFO's policy will continue as before or develop a more US-style approach in this and other regards.[18]

14 For US Deputy Assistant Attorney General Matthew Miner's Keynote Address at the 9th Global Forum on Anti-Corruption Compliance in High Risk Markets on 25 July 2018, see https://www.justice.gov/opa/pr/deputy-assistant-attorney-general-matthew-s-miner-remarks-american-conference-institute-9th.

15 https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

16 https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/. These are objective statements of position, not subjective opportunities for evaluation of specific conduct.

17 'Ethical business conduct: an enforcement perspective' – speech by David Green QC, former Director of the Serious Fraud Office (SFO), to PricewaterhouseCoopers on 6 March 2014.

18 https://globalinvestigationsreview.com/article/1173689/osofsky-%E2%80%9Ci%E2%80%99ll-be-a-different-kind-of-director%E2%80%9D.

In terms of formal statements, a party dealing with the SFO is limited to the guidance contained in judgments and agreed terms of settlement under DPAs, of which there have only been five to date, four concerning the section 7 offence under the Bribery Act 2010 of failing to prevent bribery (three of which also involved substantive bribery offences).[19] More informal statements of policy and approach have been made in speeches by SFO staff to professional audiences,[20] but these remain indicative statements of policy intent and are not analogous to the DOJ opinion procedure.

In the United Kingdom, although the Financial Conduct Authority (FCA) issues policy statements from time to time, it will not give its blessing to a product, service, contractual undertaking or other course of conduct, nor will it make available records it holds in its supervisory or enforcement capacity that companies may rely on when evaluating an intended counterparty. This reluctance is a combination of statutory obligation in relation to the management of confidential information (enshrined in the Financial Services and Markets Act 2000 (FSMA))[21] and because as a regulatory body it is subject to judicial review should it exceed its jurisdiction. Records of authorisations, published enforcement notices and decisions of the disciplinary tribunal are in the public domain, but there is no 'surgery service' to help companies determine the correct approach to the interpretation of their regulatory responsibilities relating to specific counterparty risks. Informal discussion, in the course of 'close and continuous' supervisory dialogue pursuant to a firm's Principle 11 obligations,[22] may shed light on the approach that the FCA may take, but these will not constitute formal policy guidance or policy statements to rely on for the purposes of transactional due

19 (1) *Serious Fraud Office v. Standard Bank PLC (now known as ICBC Standard Bank PLC)*, 30 November 2015, Case No. U20150854. The SFO's press release with the deferred prosection agreement (DPA) and statement of facts can be found at https://www.sfo.gov.uk/2015/11/30/sfo-agrees-first-uk-dpa-with-standard-bank/; (2) *Serious Fraud Office v. XYZ Limited*, 11 July 2016, Case No. U20150856. The identity of the defendant has been redacted from the press release dated 8 July 2016 and final redacted judgment dated 11 July 2016 pending ongoing proceedings, with the full DPA, statement of facts and full judgment due to be published when those proceedings are concluded; (3) *Serious Fraud Office v. Rolls-Royce plc and Rolls-Royce Energy Systems Inc*, 17 January 2017, Case No. U20170036. The SFO's press release with the DPA and statement of facts can be found at https://www.sfo.gov.uk/cases/rolls-royce-plc/; (4) *Serious Fraud Office v. Tesco Stores Limited*, 10 April 2017. The judgment, DPA and statement of facts can be found at https://www.sfo.gov.uk/cases/tesco-plc/; and (5) *Serious Fraud Office v. Serco Geografix Ltd*, 4 July 2019. The SFO's press release with the DPA and statement of facts can be found at https://www.sfo.gov.uk/2019/07/04/sfo-completes-dpa-with-serco-geografix-ltd/.

20 e.g., speech to the Annual Bribery and Corruption Forum by Ben Morgan, Joint Head of Bribery and Corruption, SFO, 29 October 2015, in which the principles of co-operation credit and the application of the DPA jurisdiction were further explored.

21 Sections 348 to 353 of the Financial Services and Markets Act 2000 (FSMA) govern the FCA's treatment of information provided subject to duties of confidence and include certain exceptions to restrictions on disclosure of confidential information.

22 Under Principle 11 of the FCA's Principles for Businesses, a firm must deal with its regulators in an open and co-operative way and must disclose to the appropriate regulator anything relating to the firm of which that regulator would reasonably expect notice.

diligence or otherwise. A regulated entity is left with the unenviable task of accumulating a body of know-how as to the likely FCA reaction and expectation based on its continued engagement, which is made harder by a considerable degree of personnel turnover at the regulated entity and the regulator itself.

Tensions inherent in the management of privilege and confidentiality 2.2.3

In the United Kingdom and the United States, where similar (but not identical) doctrines of legal professional privilege exist, and in civil law jurisdictions that do not recognise the concept of privilege but rely heavily on the doctrine of professional secrecy, significant pressure points arise as a company seeks to keep material privileged and confidential while also satisfying the appetite of public bodies (regulators, prosecutors and legislators) and customer or investor groups for unguarded candour. There may even be a significant strategic divergence within a company's own board and management on the balance to be struck between transparency and established legal controls. These tensions emerge in investigations and, as a consequence, in the course of corporate activity.

For the company, tension immediately arises between the various duties owed to customers, shareholders and employees, on the one hand, and the protection of the right of confidentiality as between lawyer and client on the other. Many would focus on the expectations of regulators and prosecutors in respect of valid claims to privilege, and the difference of opinion between those parties and the company as to the status of information (whether disclosable or not). Yet, it is often tension, error, omission or indecision in the company that creates the greatest scope for complexity, long before any debate with authorities or before the courts has begun.

In a transactional context, for example, a target may want to share information so that an acquiring company can assess its exposure to certain risks. The target may hold a volume of documents and information ranging from initial fact-finding witness-interview material to the conclusive investigation report into the precise issues of concern. Yet the target will fear that waiver of privilege over that material may open it up to collateral waiver risk and an inability to defend speculative discovery requests in civil claims at a later date. As such, while non-disclosure may damage the prospects of the transaction or create future litigation risk, unbridled waiver may facilitate third-party litigation down the road.

One possible solution, as an alternative to relying on the concept of a 'limited waiver', has been the application of the common interest doctrine to the disclosure to the acquirer for a specific and limited purpose.[23] An example of effective

23 In the United States, the common interest doctrine varies from state to state. Under New York law, its application is limited to communications related to pending or anticipated litigation, rather than an anticipated merger or other commercial activity. *Ambac Assurance Corp., et al. v. Countrywide Home Loans, Inc., et al.*, 27 N.Y.3d 616, 627 to 629 (2016). In Delaware, which is generally considered the leading jurisdiction for corporate law, however, the privilege is much broader. 'A client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client . . . (3) by the client or the client's lawyer or a representative of the lawyer representing another in a matter of common interest.' Del. R. Evid. 502(b)(3).

use of a common interest privilege agreement is a joint venture business (A), the main investor in which is corporation (B), which invites investment by a venture capitalist (C). A faces substantial patent litigation in relation to the underlying product, constituting a substantial risk to the viability of the business. There exists a legal opinion as to the merits, sought by A in the ordinary course of the litigation. It is privileged and confidential as against B and C, who are not parties to the action but have a common interest in its outcome as they are aligned in wanting it to fail. Their investment may even support that. This is the typical circumstance in which a common interest privilege disclosure will be made to two parties, to inform their investment decisions, who are then subject to contractual duties of confidentiality to guard against arguments in litigation over waiver of privilege.

See Chapters 35 and 36 on privilege

On these grounds the acquirer can satisfy itself that it has made a true and fair evaluation of the risk, but this still leaves open questions as to how this risk assessment can subsequently be articulated in public statements if privilege is to be maintained and how the decision to advance can be justified to investors in the absence of a subsequent waiver of privilege. There is, however, conjecture in the United Kingdom as to the balance between risk and value in the application of the common interest doctrine in circumstances where authorities suggest a limited waiver may be sufficient.[24] In the United States, the concept of limited waiver, generally, does not exist.[25]

Similarly, a regulated entity will be concerned as to how it can defend a commercial decision to a regulator without sharing the contents of a privileged document. If it does share privileged material, what is the status of that disclosure? Will the restrictions over a regulator's dealings in confidential information,[26] or a specifically worded, limited waiver be sufficient to ensure there will be no onward disclosure or gradual widening of the waiver, weakening subsequent defences to disclosure in civil or criminal proceedings? Under English law, disclosure to a regulator on specific terms as to confidentiality, privilege and entitlement on the part of the regulator to make limited onward disclosure for a specific statutory or other legal purpose would not necessarily result in a wholesale waiver.[27]

See Chapters 35 and 36 on privilege

The law applies 'especially within the context of a pending transaction' when discussion 'involved legal issues regarding the transaction'. *3Com Corp. v. Diamond II Holdings, Inc.*, No. 3933-VCN, 2010 Del. Ch. LEXIS 126, at *13, *24 & n. 18 (Ch. 31 May 2010).

24 *Gotha City v. Sotheby's (No.1)* [1998] 1 WLR. 114 confirmed that where advice is shared with another party on a confidential basis, the waiver of privilege as between them did not constitute a waiver of privilege as against the wider world. In *Property Alliance Group v. Royal Bank of Scotland* [2015] EWHC 1557 (Ch), Mr Justice Birss applied *Gotha* and confirmed that waivers of privilege can be made for a limited purpose and that this would prevent the person to whom the document was disclosed from using it in circumstances outside the limited purpose.

25 See, e.g., *Pac. Pictures Corp. v. United States Dist. Court*, No. 11-71844, 2012 U.S. App. LEXIS 7643 (9th Cir. 17 April 2012) (rejecting the theory of 'selective waiver' and holding that a party who provides attorney–client privileged materials to the government may not thereafter claim the privilege in civil litigation).

26 e.g., FSMA, section 348.

27 In *Property Alliance Group v. Royal Bank of Scotland* [2015] EWHC 1557 (Ch), the documents in question had been provided to various regulators on the basis that confidentiality and privilege

At the heart of a claim to the protection of privilege is a duty to maintain confidentiality; yet in commercial circumstances the goals of candour and transparency, the disclosure duties set out in financial reporting standards and the reasonable investor test are at odds with the goal of maintaining enforceable claims to privilege in all instances. Counsel therefore often faces the unenviable task of electing which legal risk to prioritise.

In many boardrooms, in common with the views of many regulatory enforcement teams and prosecutors, there is a growing distaste for opportune (though arguably valid) claims to privilege that may obscure a complete understanding of the facts, and increasingly a premium is placed on holding nothing back. This may see the pendulum swinging towards greater disclosure and less concern about privilege, until a company cannot protect against litigation risk that would have been defensible had privilege not been waived. In the United Kingdom this moment has not fully arrived. While debates within the boardroom may rage in relation to the value of greater transparency and the reputational dangers of over-reliance on privilege and confidentiality, there is still a legitimate reliance on the protections afforded by legal professional privilege. In turn, this is being met with a greater level of scrutiny and challenge by public authorities, and episodes of intense litigation on issues of privilege appear to be increasing. Prosecutors and regulators press for greater levels of disclosure but cannot legitimately demand waiver of privilege as a key ingredient of a co-operative dialogue. Instead, they challenge perceived invalid claims or, in the United Kingdom, encourage it as part of the 'co-operation credit' debate to which many companies contemplating a DPA are sensitive. At the same time, the decisions in *The RBS Rights Issue Litigation* and *ENRC*[28] provided further guidance on the limited extent to which materials created during an investigation may be withheld on the grounds of legal advice privilege and litigation privilege. *The RBS Rights Issue Litigation* and *ENRC* highlight, among other things, the difference between the United States' and the United Kingdom's approaches to privilege and interview notes: whereas the interview notes in question would likely have been protected under the attorney–client privilege and work-product doctrine had US law applied, they were not covered by legal advice privilege in the United Kingdom. The first decision in *ENRC* was highly controversial, in large part owing to the findings, fatal to ENRC's claim for litigation privilege, that a criminal investigation was not 'adversarial' litigation and that reasonable anticipation of a criminal investigation did not necessarily equate

See Chapter 35 on privilege

would be preserved as against third parties. The agreements with the regulators contained 'carve-outs', which permitted the regulators to share the documents with other third parties (such as other government or regulatory agencies) and to make the material public or to disclose it further. Birss J found that those carve-outs did not amount to a general waiver of privilege and stated: 'The fact that the carve-outs recognise the regulator's rights and obligations to take a step, which might go as far as even publishing the information in the document, makes no difference if that has not happened. Until they do, I fail to see why the confidentiality and privilege would not be preserved.'

28 *Re The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch); *Serious Fraud Office (SFO) v. Eurasian Natural Resources Corporation Ltd* [2017] EWHC 1017 (QB) 8 May 2017; *Serious Fraud Office (SFO) v. Eurasian Natural Resources Corporation* [2018] EWCA Civ 2006.

to the reasonable contemplation of a criminal prosecution. The *ENRC* decision was, however, challenged before the Court of Appeal, which concluded that litigation (in the form of criminal proceedings) was reasonably in contemplation at the time when ENRC had instigated its own internal investigation and that the other ingredients for litigation privilege were present. As such, litigation privilege applied to the notes of interviews with employees, former employees, company and subsidiary officers and other third parties. While the appeal decision in *ENRC* provides welcome relief in respect of the potential availability of litigation privilege in investigations, the United Kingdom remains significantly at odds with the United States on the applicability of legal professional privilege generally, which is an obvious cause for concern in cross-border investigations. Furthermore, as observed in the *ENRC* appeal judgment, the United Kingdom is also at odds with international common law in terms of the scope of legal advice privilege. Although discussion of the scope of legal advice privilege featured in the *ENRC* judgment, the Court of Appeal was clear that any re-examination of the ambit of legal advice privilege must be left for the Supreme Court.

In the United States, where prosecutorial demand for privilege waiver for a corporation to receive full co-operation credit was once common, federal prosecutors may no longer ask for a waiver of the privilege, although corporations must disclose all relevant facts, including against its employees, to receive co-operation credit.[29] Further, the fact that a corporation does not waive the attorney–client privilege during a government investigation cannot be used against a corporation when determining whether it 'co-operated'.[30]

In practical terms there is some hope for reconciliation of these conflicts by creating separate documents during the investigation: reports to management containing legal advice on investigative outcomes (privileged) having a separate purpose to reports of findings to regulators (not a privileged purpose). Additionally, facts themselves are not privileged[31] and may be presented to law enforcement and regulators, with careful handling to present them as only facts and not the product of specific counsel interviews, without waiving the privilege.[32] In the United Kingdom, fact-finding interviews can be conducted on the basis that the interviewee is not the client and the purpose of the interview is not the giving or receiving of legal advice (consistent with the decisions in *The RBS Rights Issue Litigation* and *ENRC*), working on the assumption that notes of the interview will not be privileged communications and should be drafted with that

See Chapter 35 on privilege

29 JM § 9-28.710–9-28.720.

30 Id.

31 See *Upjohn Co. v. United States*, 449 U.S. 383, 395-96 (1981).

32 See *United States v. Stewart*, No. 15CR287, 2016 U.S. Dist. LEXIS 103516, at *5 (S.D.N.Y. 22 July 2016) (in-house counsel waived privilege over defendant's communications by disclosing them to the Financial Industry Regulatory Authority, because counsel's disclosure contained not only unprivileged facts, but also the contents of privileged communications, i.e., counsel's questions to the employee).

in mind.[33] In the United States, however, the same material may be covered by the attorney–client privilege and work-product doctrine.[34] This presents a significant legal and practical concern in the management of transatlantic investigations, as it raises the threat of subject-matter waiver in the United States.[35] *Ex post facto* advice to management on the content or outcome of interviews, however, is likely to attract privilege. Yet, ultimately, there may be a point of strategic principle for a board and its advisers to determine: to waive or not to waive.

Whistleblowers, complaints and concerns 2.2.4

While certain investigations will be triggered by established controls or 'accidental' awareness of conduct risk, a very substantial proportion of matters under investigation will be instigated by virtue of a company's policy and practice on raising concerns, namely staff exit interviews, employee helplines and voluntary communications by staff, customers, former employees and members of the public. Together these forms of communication fall into a single, growing class of investigation trigger: whistleblowing.

Whistleblower complaints present a significant overhead for a company, in both financial and reputational terms. The number of complaints received does not necessarily determine how 'healthy' an organisation is as regards conduct risk; a significant flow of concerns may indicate a more risk-aware body of employees who feel free to challenge or raise issues without fear for their future employment. The key data is in the nature of allegations and the extent to which points raised are substantiated.

There are a series of primary investigative goals, before the underlying facts are conclusively determined. These are (1) the assessment of the credibility of the complaint and complainant (establishing whether it is a *bona fide* concern, and whether the matter has been previously raised and determined), (2) the duty owed to the complainant and any other parties in the circumstances (confidentiality and other safeguards of persons and evidence), and (3) whether a full investigation is necessary and, if so, the precise extent of allegations under investigation. Many

33 Note, however, that if the test for litigation privilege is met, interview notes may be covered by litigation privilege.

34 See, e.g., *SEC v. Roberts*, 254 F.R.D. 371, 375 (N.D. Cal. 2008); *SEC v. Schroeder*, No. C07-03798 JW, 2009 U.S. Dist. LEXIS 39378, at *20 (N.D. Cal. 27 April 2009); *Nat'l Union Fire Ins. Co. of Pittsburgh, PA v. AARPO, Inc.*, No. 97-CV-1438, 1998 U.S. Dist. LEXIS 21342, at *4 (S.D.N.Y. 24 November 1998); see also *City of Pontiac General Employees' Retirement System v. Wal-Mart Stores Inc, et al.*, Case No. 5:12-cv-5162 (W.D. Ark 2012), Order 5 May 2017. An internal investigation conducted by non-lawyer investigators, not under the direction of counsel, nor in contemplation of litigation, is protected by neither the attorney–client privilege nor the work-product doctrine.

35 The Federal Rules of Evidence state: 'When the disclosure is made in a federal proceeding or to a federal office or agency and waives the attorney–client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a federal or state proceeding only if: (1) the waiver is intentional; (2) the disclosed and undisclosed communications or information concern the same subject matter; and (3) they ought in fairness to be considered together.' Fed. R. Evid. 502(a). As interpreted, Rule 502(a) generally tends to narrow the scope of waiver.

companies will have clear policies on handling whistleblower complaints, but different companies and jurisdictions will apply varying standards and expectations as to the treatment of complainants. Some principles of general application are nonetheless emerging, namely:

- Whether complainants are actually whistleblowers if they do not class themselves as such is a matter that can be objectively assessed; it is the nature and context of the concern raised, and the policies and procedures triggered by those concerns, that determine the duty owed to them (such as a right to anonymity, the duty to report to authorities, employment protection and so on).
- How the concern is raised does not determine it as whistleblowing. The issues do not have to be raised in correspondence, through a helpline or formal complaints log: concerns can be raised orally in exit interviews, in informal email correspondence, during tribunal proceedings, by voicemail or in passing in social conversation in the office.
- A sensible rule of thumb is to ask whether the substance falls into the categories either defined in the policy on raising concerns or, in the unlikely event of there not being one, whether it constitutes the form of concern or complaint that a regulator would expect (or best practice would require)[36] to be treated with the controls and protections afforded to a whistleblower.
- In cases of doubt, the rights of the individual to protection should override the interests of the company such that complainants should be treated as whistleblowers and afforded necessary protection until the issue is clarified.
- There has been increased focus on the importance of protection of those raising concerns, including ensuring no steps are taken to identify those complainants seeking or entitled to anonymity. The FCA and the Prudential Regulatory Authority have reiterated their expectations as to the appropriate management of complainant confidentiality and the duties owed by regulated sector companies and individuals.[37]
- Care should nonetheless be taken to distinguish between genuine whistleblower cases and the raising of grievances contrary to process, although some allegations may be so significant or toxic to the company's reputation and financial interests that even an issue arising in an employment context but raised inappropriately or otherwise resolved may need to be investigated (e.g., an allegation of bribery made notwithstanding the existence of a compromised exit).
- A whistleblower may be the source of an allegation but need not (and probably should not) be involved in steering process or in determining or influencing the strategy or outcome. There is no obligation to provide a whistleblower with information in relation to findings, and there may be a significant downside in doing so in terms of loss of privilege and confidentiality. However, a

36 e.g., in guidance by unions, professional bodies or other interest groups or charities such as, in the United Kingdom, Public Concern at Work (www.pcaw.org.uk/).

37 See https://www.fca.org.uk/news/press-releases/fca-and-pra-jointly-fine-mr-james-staley-announce-special-requirements.

whistleblower should be made aware that the allegations have been taken seriously and are being addressed.

- Loss of *bona fide* status (e.g., in circumstances where spurious allegations are made for financial gain, employment protection or to blackmail) may result in the individual losing enhanced 'whistleblower' protection,[38, 39] but this must be contrasted with jurisdictions encouraging whistleblowing through 'bounty' schemes such as that offered by the US SEC's Office of the Whistleblower that do not impose any good faith requirement on the bounty recipient.[40]
- Bounty schemes and similar arrangements may influence the jurisdiction in which matters are first raised, but a company cannot rely on regulatory issues staying within that jurisdiction. As noted above, regulatory information gateways provide for the sharing of information between regulators and prosecutorial authorities in different jurisdictions (e.g., between the FCA and SEC, and between the DOJ and the SFO). As such, there should be an assumption of wide knowledge.
- Whistleblower initiatives are slowly gaining traction across the globe. A number of regulators (such as the IRS and SEC) in the United States in particular have established practices. However, there are significant cultural differences and enhanced data protection laws in certain European jurisdictions (particularly those whose current laws reflect the reaction to the intrusions of secret intelligence services in the 20th century, and where it is necessary to respect the legitimate reasons why these countries may continue to wrestle with the idea that staff should be encouraged to report colleagues' misconduct). There are some active reward programmes in Europe, such as the UK Competition and Markets Authority offering rewards of up to £100,000 for information on cartel activity, although these are much more limited than the incentives available in the United States. In October 2019, however, the European Union adopted a Directive on the protection of persons who report breaches of Union law,[41] which may encourage more whistleblowers to come forward. The new rules

See Chapters 19 and 20 on whistleblowers; see also Vol. II chapters at question 28

38 In the United Kingdom, the Public Interest Disclosure Act 1998 sets out protections for whistleblowers who are dismissed or affected as a consequence of making a disclosure as a whistleblower. Section 17 narrows the definition of protected disclosures to those made 'in the public interest'. Section 18 provides that tribunals may reduce compensatory payments in circumstances where the disclosure was not made in good faith.

39 In the United States, one eligibility requirement for whistleblower retaliation protection under the Dodd-Frank Act is that the whistleblower report conduct he or she 'reasonably believes' constitutes a violation. 18 U.S.C. § 1514A(a)(1). The employee's 'reasonable belief' must be both subjectively and objectively reasonable, and a good faith requirement has been interpreted as part of subjective reasonableness. *Day v. Staples, Inc.*, 555 F,3d 42, 54 (1st Cir. 2009); *Ashmore v. CGI Group Inc.*, 138 F. Supp. 3d 329, 344 (S.D.N.Y. 2015).

40 Pursuant to the Dodd-Frank Act, the SEC provides monetary awards to individuals, providing they meet certain criteria, who provide information leading to an enforcement action in which over US$1 million in sanctions is ordered. Awards range from 10 to 30 per cent of the amount collected. See https://www.sec.gov/whistleblower/.

41 See https://www.consilium.europa.eu/en/press/press-releases/2019/10/07/better-protection-of-whistle-blowers-new-eu-wide-rules-to-kick-in-in-2021/.

require (1) companies to create reporting channels and (2) a response within a fixed timescale. EU Member States will have two years from publication in the European Union's Official Journal (expected in late 2019) to comply. Outside the European Union, Australia's new whistleblower protection laws became effective in July 2019, requiring companies to have a whistleblower policy from January 2020.[42] However, the importance given to information from whistleblowers, the protection they are afforded and, accordingly, their willingness to come forward, vary widely across the world.

2.2.5 The role of the internal audit function

Many companies do not have (whether as a consequence of funding limitations, strategy or structural considerations) free-standing internal investigations capability. Some will have delegated that responsibility to the internal audit function. Even within that sector, which does have specific investigative capability, there may be examples of investigations having been undertaken by the internal audit functions as part of their ordinary control function activity. As internal investigation capability and practice have grown as a priority for business, so has the recognition that this is not the role of an internal audit function.

In a well-governed business, the purpose of internal audit is to provide the board with independent objective assurance as to the effectiveness of the enterprise-wide control framework. In summary, this means the identification of the appropriate controls in respect of specific (financial and other) risks and the assessment of their efficacy: identifying the risk to which the control relates; identifying the risk 'owner'; measuring the effectiveness of the control; mandating improvements where breaches or weaknesses are observed and escalating material control weaknesses to senior management or the board as necessary; tracking remedial action; and assessing the improved control environment. The DOJ's guidance on the evaluation of corporate compliance programmes asks companies to query how often internal audits are conducted in high-risk areas, whether the company audited its compliance programme and what control tests the company has generally undertaken.[43]

These activities are closely connected to, but not synonymous with, investigations. Internal audits are systematic reviews of the group-wide risk control framework and are not event-driven. They do not concern themselves with the investigation of complaints or claims with free-ranging subject matter or context, but are limited to the structure of the control framework devised by senior management.

Internal audit is not part of a legal function providing advisory services, so the output is not subject to legal privilege as a matter of English law (even where audit staff may be legally qualified, they are not tasked with providing legal advice to a client). In the United States, there is a practical refinement: where for a particular

42 See https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/.

43 US Department of Justice, Evaluation of Corporate Compliance Programs, § 9. See https://www.justice.gov/criminal-fraud/page/file/937501/download.

exercise members of the internal audit team are designated as working under the direction and control of the legal department, as its agent, for the purpose of providing expert assistance to the legal department in rendering legal advice to management then privilege will attach to their communication.[44] In the United Kingdom, this may be theoretically possible in circumstances where the audit team forms part of a working group under the control of a legal counsel or team, yet the very distinct role differentiation between audit and legal functions in UK corporate governance makes this a hard argument to sustain. Usually, an audit report that addresses legal issues, setting them out with clarity, identifying the controls, possible breaches and remediation recommended, and then identifying a lack of action in response to the recommendation can present dangers for an organisation. The report will be an unprotected disclosable document that presents a regulator, prosecutor or civil litigation claimant with a perfect platform – a charter for enforcement or a document undermining the credibility of a defence in a civil action. But this is not to suggest that internal audit has no role in internal investigations. On the contrary, it is one of the most important company functions, yet the timing and structure of its involvement in investigations is critical.

Internal audit output permits a pre-emptive, focused approach to investigation that is not simply limited to the complaints and concerns raised but operates within a risk-based evaluation culture. Internal audit reports allow a group-wide perspective on control weaknesses that enables investigators to concentrate resources in the most pressing areas of concern (whether in terms of reputational or financial risk) to the board, as opposed to responding piecemeal to each issue as it presents itself. This is important for an effective investigation function, as successful performance generates greater reliance and workloads can escalate aggressively once business leaders identify the value it can deliver. An internal audit function can therefore help to align an investigative function's input and output with the business's strategic risk management agenda.

Internal audit activity can also coincide with investigations, with the two functions reviewing similar subject matter, each with distinct purposes, strategies and methodologies, creating the obvious danger of conflicting or partly inconsistent outcomes (at least one of which will not be a privileged document and may contain stark conclusions in relation to the cause of a control breach). An internal audit, ideally, should occur subsequent to an investigation and may even rely on the contents of an investigators' report to focus the audit process. However, audit programmes tend to be cyclical, thematic or random, and internal auditors are understandably resistant to pressure from any part of the company to suspend or reschedule a standard audit (as this itself could constitute a breach of policy or control deficiency). Enhanced levels of communication between functions may assist in avoiding this risk, but a clash may be inevitable.

What steps can be taken to mitigate this risk? It may be possible to argue that audit is a limited process for a specific purpose, and not a comprehensive factual

44 See *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).

review. Investigation reports do have to distance their findings from time to time from historical and problematic, strident or oversimplified audit reports, and this can cause an issue where there are different findings on the same or similar facts in close proximity to each other. A forensic investigation is likely to be more comprehensive as it is likely to have included a wider range of evidence, including document reviews, e-discovery and, crucially, witness interviews. Furthermore, lawyers may be able to obtain more detail in the course of a formal interview dialogue where witnesses consider the implications of their responses more than in a control assurance review. It is essential, therefore, that the scope and purpose of an investigation be distinguished at the outset from a narrower control review or audit.

2.2.6 The role of the compliance function

A number of the observations above in respect of internal audit apply equally to the compliance function and are not repeated here. The standard control environment model is a three-legged stool: legal, compliance and risk, each with distinct but collaborative functions, with internal audit acting as a monitor separate from those operational controls. While positioning investigative capability within the legal function maximises claims to privilege and creates the opportunity for deploying the forensic expertise of litigation lawyers in investigative roles, it is by no means standard in the market, and many companies still engage compliance teams in investigative activity. The advantage is the natural connection between investigation, control assurance, control remediation and regulatory liaison, but the separation of roles avoids the risk of conflicts of interest (where, for example, a compliance function has been responsible for implementation of controls and measurement of their effectiveness, but is then charged with investigating breaches and establishing personal accountabilities).

As compliance functions are developing, particularly in the regulated financial services sector after the global financial crisis, a consensus is developing within companies and regulators that the proper home for conduct risk, whistleblowing and certain categories of investigation is the compliance function. There is an increasing pattern of financial crime risk management (policy ownership for bribery and corruption, money laundering, sanctions) being owned by the compliance function, and this has led a significant proportion of companies to extend the responsibility for investigation of these areas to compliance teams as well.

There is, however, a significant difference between ownership of policy and risk, on the one hand, and investigation of a suspected breach on the other, and significant governance concerns arise where the owners of a risk investigate the adequacy of their own conduct. For example, initial public criticism of banks' handling of issues over the London Inter-Bank Offered Rate (LIBOR) focused on the decision within some firms not to escalate concerns beyond the compliance function or the conduct of inadequate, early investigation by compliance teams within the affected businesses lines. Independent legal teams then proceeded with more thorough investigation of the issues, benefiting from the application of privilege where applicable (noting the points above and in Chapter 35 in relation

to *The RBS Rights Issue Litigation* and *ENRC* decisions) as well as acting independently of the business. Learning from this episode, a number of banks restructured their compliance functions, separating the three legs of the stool more emphatically. They created greater levels of governance and control as between the respective functions, with operational framework agreements in place to ensure formal triggers for referral from compliance to legal in certain circumstances where the value or subject matter identifies a level of enhanced legal risk (e.g., bribery and corruption, financial sanctions, high-value fraud, or other systemic control breaches that could have material financial or reputational implications).

Considerations for investigations triggered by external events 2.3

Contact by authorities 2.3.1

In the UK regulated sector, where open and transparent supervisory dialogue is expected, it is comparatively rare for a business to find out about issues for the first time as a result of unilateral contact from a regulator. Ordinarily the regulated entity's report to the regulator leads to further investigation. By contrast, however, contact from prosecutors, competition authorities and, in certain circumstances, civil litigants may occur without prior warning. In the United States, corporates frequently learn of an investigation for the first time from prosecutors, and criminal referrals from regulatory agencies to the DOJ are common. The following does not seek to list all circumstances in which contact from authorities may trigger investigation, but it highlights certain aspects of unsolicited contact that may raise legal concerns.

The first challenge for a company is to discern the nature and purpose of the authority's enquiries, and in particular to distinguish between an investigation by a regulator and one by a prosecutor. While a company may be inclined to treat the two forms of organisation as synonymous, they are not. They discharge different duties, carry different powers (although they sometimes overlap) and have different expectations regarding co-operation. Accordingly, a company's approach to dealing with a regulator may differ from its response to a prosecutor.

A prosecutor investigating a matter is normally seeking evidence to decide whether a crime has occurred and whether individuals or the company should be criminally charged. If it proceeds with a prosecution, it carries the burden of proof (with certain limited jurisdictional and subject-matter exceptions). Apart from specific mandatory reporting regimes,[45] there is no obligation to volunteer information about misconduct to a prosecutor in the absence of a subpoena, warrant or other court order. It is an offence to obstruct an investigation, but obstruction does not extend to failure to volunteer evidence in the absence of compulsion; however, the provision of false, misleading or incomplete information to a prosecutor could amount to an offence of obstruction of justice in the United States or perverting the course of public justice in the United Kingdom. In the

See Chapters 5 and 6 on beginning an internal investigation

45 e.g., the obligation in the United Kingdom to submit suspicious activity reports under section 330 of the Proceeds of Crime Act 2002.

United States, it is a crime to destroy evidence, even in the absence of compulsion or the initiation of a proceeding, when the purpose is to avoid its disclosure in an anticipated criminal or regulatory investigation or proceeding.[46] Further, the Fifth Amendment right against self-incrimination extends only to individuals, not corporations. Therefore, ancillary Fifth Amendment protections, such as the act of production doctrine, which permits an individual to hold back documents if the mere act of producing them, as opposed to their content, will be incriminating, does not apply to corporates.[47, 48]

In dealings with UK prosecutors, while opportunities for mitigation and leniency exist through demonstrable co-operation[49] (and a company may regret not being able to obtain co-operation credit later on), co-operation is a matter of pragmatic choice rather than legal obligation. The starting point remains unchanged: under what valid power does the prosecutor seek the evidence, what are the company's reasonable defences and how tactically does the company respond? While principles of co-operation with government agencies in the hope of gaining leniency or mitigation are more clearly defined and have a longer tradition in the United States, the general rule of law remains intact and questions of powers, defences and tactics are no less germane.[50]

Where a prosecutor, police or investigative agency, competition authority or other public body serves a subpoena, order or warrant entitling it to documents and electronic information, or to enter, search and seize, monitor or restrain, the challenge for the affected organisation is twofold: (1) to provide information or permit access and activity within the confines of the power granted; and (2) to ensure the company is not left behind (and preferably remains in front) in its own understanding of the relevant facts.

See Chapter 11 on production of information to authorities

In the United States, grand jury subpoenas are the most common tool prosecutors use to gather information against a corporation in a criminal investigation. Various civil and regulatory enforcement agencies, such as the SEC and Commodity Futures Trading Commission, may also issue subpoenas. General principles to follow when responding to a subpoena include issuing hold notices to the relevant employees and, if appropriate, third parties, to ensure that all

46 See 18 U.S.C. § 1519.

47 See *United States v. Hubbell*, 530 U.S. 27 (2000).

48 For the UK financial services industry, this is to be contrasted with the duty of open and co-operative dealings with the FCA, whereby evidence of a control breach would be reported without delay and significant regulatory implications could arise from a failure to do so. A US corporate's duty to disclose is limited. See Chapters 9 and 10 on co-operating with authorities.

49 In the United Kingdom, with the introduction of the Serious Fraud Office's DPA power in 2015.

50 There is no legal obligation to co-operate in an investigation in the United States. Under the Principles of Federal Prosecution of Business Organizations, however, a corporation's willingness to co-operate is a factor in determining whether to charge the corporation. But, a corporation's refusal to co-operate alone is not justification for prosecution. See JM § 9-28.700. Formal obligation aside, from a more pragmatic perspective, US and UK entities under a DPA or NPA, or parties subject to monitorships, may find they have little choice but to disclose, as might a member of the heavily regulated financial services sector, which could face adverse findings in relation to the duty to deal openly and transparently with its regulator.

information requested or potentially relevant to the enquiry (emails, other electronically stored information, hard-copy documents, etc.) is retained; controlling insider lists to identify those now aware of facts that may constitute inside information; preparing witness lists (to ensure they do not receive updates or advice on the matter, which may contaminate their evidence); and giving consideration to the treatment of witnesses (whether they require independent legal advice, or should be removed from the office environment through suspension or relocation so as not to risk evidence tampering, collusion or undue influence over other witnesses). In a criminal matter, defence counsel will almost always engage with the prosecutor to determine the company's status as a witness (potentially having relevant information, but no criminal liability), subject (the largest category, in which the government does not yet have sufficient information to determine criminal liability) or target (the government is gathering evidence to bring criminal charges against the company).[51] Counsel will also almost certainly work to narrow the scope of the information requested.

A number of important general principles apply also to the execution of search warrants and the conduct of dawn raids:

- The order or warrant must be reviewed to ensure that the party serving or executing it has the requisite power. (Does it catch the correct entity? Is it the correct site or office? Are the search area and the items the authorities are searching for described with the requisite particularity? Are there date or time discrepancies? Is it signed or executed? In the United Kingdom, does it bear the correct court seal? Does the person conducting the inspection have the requisite authority in that jurisdiction?)
- All relevant parties need to ensure the full scope and context of the search is understood (and where electronic searches are undertaken, endeavour to agree on relevant keyword searches and the exclusion of out-of-scope material, such as privileged documents or personal data).
- As with a subpoena, it will generally be necessary to issue hold notices immediately after receipt of the order or warrant with instructions not to destroy or spoil evidence or to give false or misleading information. As well as the obvious practical importance of preserving relevant evidence, there is also significant value in being seen to co-operate as an initial response.
- Individuals executing the order should be subject to identity verification to ensure that execution is in accordance with the terms of the order and that their identification is recorded (in the event that the order is breached and an individual's identity becomes relevant to any proceedings arising as a consequence).
- Staff, including reception and a designated dawn raid team, should be trained in advance as to how to conduct any interaction with investigators from the moment of first access to the premises. This includes training and instruction on not answering apparently casual questions on the subject of the

51 See also, JM § 9-11.151, defining 'target' and 'subject'.

search. The informal question to the unready on the walk along the corridor is a well-established source of information for experienced investigators. Any questions asked of staff should be noted. Employees may be informed of their legal rights not to speak to investigators and their right to counsel. Additionally, if the company is willing, the employees may be told that the company will provide legal counsel to them at no cost if investigators wish to speak to them or if they are later contacted. The company may not, however, instruct employees not to speak to investigators. That is the employee's choice.

- A separate room should be set aside as a base for investigators and discussions between legal function representatives and the visitors so that debate and investigative activity does not take place within earshot of those under investigation.
- Local IT support (technology, plus a nominated IT representative) should be made available in the same room to ensure the IT environment can be explained to investigators and accessed. A log of access and copies of materials reviewed or seized should be made as the matter progresses so that a company's own investigators and lawyers can subsequently review the same material and evaluate compliance with the order or warrant.
- A written log should be kept of all places searched and items seized. Legal counsel should be present, if possible, to assert objections based on the attorney–client privilege, to identify commercially sensitive information or the sensitive personal information of customers or employees and to object if the search exceeds its authorisation. None of this, however, can be obstructive. The remedy for an improper search or seizure is to be had in court, not while the search is being conducted.
- Seek to agree with the investigators in advance on the definition and scope of principles such as legal privilege, commercial confidentiality, relevance, personal data and other material the company would contend falls outside the terms of the order, and to a protocol for handling these materials during and after the search.
- Consider whether it is necessary and appropriate to prepare a press release or public disclosure (e.g., stock exchange announcement) confirming the on-site inspection and its scope or purpose. In the United States, it may be advisable to convene a 'town hall' meeting with employees to discuss the search and the looming investigation, but in the United Kingdom, this practice is not favoured as it could tip off individuals who do not intend to comply, triggering evidence tampering or impacting the integrity of witness testimony.

See Chapters 37 and 38 on publicity

2.3.2 External whistleblowers

Many of the points in Section 2.2.4 on internal whistleblowers apply equally to whistleblowers from outside the organisation. There are, however, further legal sensitivities in dealing with external sources of concern that merit consideration.

While an employee cannot be prohibited or discouraged, contractually or otherwise, from reporting concerns to regulators or law enforcement, an employee will probably otherwise be subject to a contractual duty of confidentiality in respect to matters arising within the company and may often have a sense of

loyalty to the company. Hence an internal whistleblower presents a more limited threat of public or further disclosure than an external whistleblower. Where an employee does not respect his or her obligations, care should be taken on the issue of enforcement of contractual and other duties of confidentiality, as a first response that apparently seeks to silence someone speaking up can appear extremely unattractive to the media, regulators and other authorities.[52] This has, more recently, become very sensitive in the context of sexual assault and discrimination claims and campaigns initiated by whistleblower complaints – including the #MeToo movement – with an increasing number of organisations publicly stating that they will not enforce confidentiality undertakings against complainants who are victims of such conduct in the workplace, notwithstanding their presence in employment contracts and compromise agreements, or choosing not to include them in newly executed agreements.

External whistleblowers frequently adopt a multi-level strategy for ensuring their concerns receive attention. First, they communicate through the formal whistleblower route, challenging the company to demonstrate the efficacy of its response. At the same time, or shortly after, they write directly to the board, senior management and shareholders, frequently copying in other third parties. Frustrated by inaction, they may turn to media interviews to increase pressure. Communication with regulatory authorities and other public bodies may follow.

It may be tempting to regard these scattergun approaches as self-evidently undermining the credibility of the issues raised and the complainant, but they are in fact remarkably effective strategies for ensuring the matter receives urgent attention, and the tools at hand for stopping wider publication are limited. Injunctive relief rarely succeeds in the face of a public interest justification.

Dialogue with the whistleblower, giving the clear impression that the company is grateful to the person for having spoken up and that an investigation is now under way, helps to reduce wider dissemination risk or slows the timetable. However, this must be balanced with the need to avoid encouraging the whistleblower to believe he or she is in charge, will be informed of the outcome of the investigation or in some way will influence the company's strategy in dealing with the issues.

A helpful counter to the lack of control a company has over the conduct of external whistleblowers is the lack of access they have to company confidential material and staff. By the same token, however, the company has limited line of sight into external whistleblowers' dealings with third parties, including public authorities. It is, therefore, advisable to invite the whistleblower to meet or speak

52 See e.g. *SEC v. KBR*, Release No. 34-74619 (1 April 2015) – fining and imposing remedial relief against KBR for violating Rule 21F-17, which prohibits impeding an individual from communicating directly with the SEC staff about a possible violation of the securities laws. KBR's violation stemmed from it requiring employees to sign confidentiality agreements as part of internal investigations, stating that they would not disclose interviews or the subject matter of interviews or investigations to anyone without the KBR legal department's prior approval, threatening disciplinary action up to termination for breaching the confidentiality agreement.

with a member of the legal function to establish what he or she knows, has done so far and is intending to do next.

Finally, internal and external whistleblowers may have protected status, whether as employees or former employees under various EU, UK and US laws, or as a consequence of a company's policy and practice. Whether or not they are protected as a matter of law, it is essential that all whistleblowers are, and are seen to be, immune from retribution. This requires the application of significant care in the treatment of their complaints, evidence, the handling of witnesses, their anonymity (whether or not requested) and the reporting of facts within the organisation, recognising that ordinary line-reporting duties may be suspended to protect the identity of the whistleblower and avoid reprisal.

2.3.3 Media coverage

Unexpected media reports or more aggressive or intrusive media behaviour (such as undercover investigative journalism) can trigger an investigation in extremely pressurised circumstances. The media body running the story will often have completed its investigation before the company is aware of the matter. In the worst cases, the first a company learns of the facts is in the publication or broadcast, although various broadcasting codes and voluntary editorial principles encourage the opportunity for a right of reply, so most coverage will follow a short period of discussion of content between the media and the subject of the story, yet not enough to accommodate an investigation and fully informed response. The company's investigation is therefore under time pressure from its first step, with media, customers, shareholders, regulators and government agencies pressing for answers or redress before the company's senior management has been able to evaluate the facts or take advice on the risk they present.

Even if it has been aware of the broader issue, and is undertaking some form of investigation, sudden and intense media scrutiny can require a company to adjust the level of response to be seen to understand public demand for resolution. Companies that were otherwise intending to adopt a more passive approach, or undertake low-key investigations and adopt a reactive media and customer stance can appear to be on the back foot as they scramble to intensify investigative efforts.

All of this can, of course, play out as complaints and concerns become part of a viral episode through social media, reducing timelines to hours and days, not weeks and months. From a practical point of view, there is an immediate balance to be struck between thorough investigation and a sufficient grasp of the facts to allow the company to demonstrate a clear strategy that can be articulated publicly (consider, for example, the initial days of the Deepwater Horizon accident in the Gulf of Mexico in 2010).

Above all, these pressures require strong triage skills and pre-existing crisis management and investigations governance, which allows incident response, investigation, legal risk management, media, shareholder and customer relations strategies to follow well-practised routines so that precious time is not taken up debating who is leading and what the right first step may be. Setting up an investigations steering group and having effective policies and processes in place that

are respected by senior management will ensure that emergency investigations are not obstructed by administrative chaos.

Customer and competitor complaints and regulatory response 2.3.4

As well as direct complaints to the company and civil litigation (which trigger the fact-gathering process), customers and competitors may refer complaints to regulators, consumer bodies and ombudsmen. Individual incidents may be sufficiently problematic to merit investigation in their own right. However, even with low-value customer complaints there comes a point where a volume of similar-fact criticisms raise concerns as to the fairness of underlying sales processes and adequacy of complaints handling systems, or perhaps even broader questions of breaches of systems or controls, that may combine to catch a regulator's attention.

While it might be hoped that a company's own monitoring of complaints levels and sources should trigger deeper investigation into the underlying issues, it will sometimes take unilateral regulatory enquiry and enforcement processes to bring about a non-voluntary, full evaluation, including thematic reviews, 'skilled persons appointments',[53] market studies and industry sweeps. Such investigations will have a significant distinguishing feature: the company's in-house investigators will not set the parameters of the investigation (though they can add significant value in debates with regulators over scope and process and may be heavily involved in the activities that follow, by partnering the external firm in a skilled person's review, for example). The in-house function will remain critical in the parallel process of evaluation of evidence as it comes to light so that advice may be taken to develop a response to regulatory or legal liability.

The influence of political agendas 2.3.5

The regulatory agenda is often set, adjusted or inflamed by the political climate, such that external regulatory or criminal investigations would not commence but for political pressure or the sudden availability of funding. The political agenda itself may change overnight in the face of public or media pressure.

Take, for example, UK parliamentary politics in the wake of the LIBOR regulatory settlements in the summer of 2012. Prior to the announcements that summer, the former Director of the SFO, Richard Alderman, had declined to commence an investigation into LIBOR manipulation citing insufficient resources to pursue the matter following budget cuts and a concern that the SFO might duplicate efforts by the Financial Services Authority and the Office of Fair Trading, which he considered better placed to determine the issues. He stepped down in April 2012 and the issue came to the public's attention in June 2012 when the first regulatory settlements were announced.

There followed a period of intense criticism in the media, growing public outcry and then questions in the House of Commons in late June 2012 as to why the SFO was not investigating the issues. Shortly after the Prime Minister's

53 FSMA, section 166.

appearance in the House of Commons to answer questions on the issue, the Chancellor of the Exchequer announced that emergency funding was being made available, and on 6 July 2012 the SFO announced it was commencing an investigation. While the banks in question had either resolved matters with their regulatory bodies or were in the process of doing so, they then faced parallel investigations into the same matters (but on a different, criminal footing concerning the conduct of individuals as opposed to the regulatory breaches by the corporations). Formal requests for witness evidence were served in the weeks and months following. Prosecutions of individuals followed in 2015 and 2016 and continue in the United Kingdom and United States.

Although banks had already conducted their own investigative activity – in certain cases some years prior to the individual prosecutions – the purpose and nature, timescale and outcomes of the SFO's enquiries were different from the regulatory investigations by UK, US and other prosecutorial authorities, and different again to the multiple competition authority enquiries on the same issues that had already occurred, requiring a flexibility in approach by banks' investigations teams, not to mention significant capacity to handle such large-scale and long-running matters.

2.3.6 Investor complaints and shareholder derivative lawsuits

While this section considers the external causes of investigations, and complaints and claims by investors may appear to fall more obviously into the 'litigation' than 'investigations' workload for a company, claims and complaints are rarely so neatly delineated. The reality for many companies is that allegations raised by shareholders can trigger twin legal activities: a defence strategy in cases where issues of liability are plainly articulated and facts are either already established or may be simply assessed; and separate investigations into wider concerns raised by the complaint, or where the facts are far from clear and the allegation cannot be adequately responded to without an investigation.

A major sensitivity in matters of this nature, which can be overlooked in pursuit of the defence of the civil action, pursuit of the HR agenda and rebuttal of individual shareholder complaints, relates to the ongoing disclosure and transparency obligations arising from stock exchange listing rules. It is one thing to investigate sufficiently to position a company to defend litigation on the balance of probabilities, or to be able to respond to a letter of concern or questions from the floor in an annual general meeting, but another to investigate to a point where a public statement can be made with sufficient accuracy to satisfy the reasonable investor test.[54]

While a company may wish to respond speedily to concerns raised by an investor, and in other circumstances considered above a 'triage' approach

54 In the United Kingdom, information a reasonable investor would be likely to use as a basis for his or her investment decisions. See the FSMA and Article 7 of the Market Abuse Regulation relating to inside information. These provisions require a high degree of precision in the accuracy of factual statements.

enables early management of matters under investigation, dealing with investor complaints carries a further layer of complexity and a balance needs to be struck, in risk-management terms, between the urgency to make a statement to the market and the time it may take to investigate facts sufficiently to permit that statement to be adequately precise and informative. The publication of false or misleading statements through inadequate or incomplete investigation simply increases the range of potential legal liabilities and further delays resolution.

Competitor complaints 2.3.7

A final category of external trigger is the complaint by a competitor (whether directly to the company or to a regulatory or criminal authority that then notifies the company).

On first analysis this seems to be little different from any other external trigger, but a complaint or concern raised by a participant in the same market raises a number of wider risks that impact the complexion of the subsequent investigation. In certain ways a competitor complaint has more in common with whistleblowing (and may even be regarded as such by authorities) in that it may create forms of protected disclosure, confidentiality obligations and behavioural expectations from particular authorities. This is certainly the case in competition matters where leniency or immunity is sought following a self-report to a competition authority following a tip-off or complaint by a competitor. This immediately limits the scope for communication of issues (including even the existence and subject matter of the investigation) among staff and will have a particular bearing on the management of evidence, including witness handling and interview processes. It will also affect the extent to which there may be ongoing communication outside the organisation where, for example, witnesses may exist within the competitor organisation but further dialogue is not possible without the consent of, and careful choreography by, the relevant authority.

3

Self-Reporting to the Authorities and Other Disclosure Obligations: The UK Perspective

Judith Seddon, Amanda Raad, Sarah Lambert-Porter, Chris Stott and Matthew Burn[1]

3.1 Introduction

Whether, when and how a company should report potential misconduct requires an increasingly 'global' (in all senses of that word) view of the risks and benefits involved. Around the world, enforcement actions in relation to bribery and money laundering are on the rise, international co-operation between authorities is being expanded and enhanced, and a growing number of jurisdictions are moving towards deferred prosecution agreements (DPAs) and formalised or protected whistleblowing regimes, as part of a general and growing trend towards incentivising corporate self-reporting.[2]

A corporate's voluntary decision to self-report requires directors to evaluate the potential benefits and risks involved in doing so, while complying with their duties under the Companies Act 2006 to consider and act in the best interests of

1 Judith Seddon and Amanda Raad are partners, and Sarah Lambert-Porter, Chris Stott and Matthew Burn are associates, at Ropes & Gray LLP in London.

2 In Lisa Osofsky's first speech as Director of the Serious Fraud Office (SFO), she referred to how the 'increasingly multijurisdictional and complex' nature of SFO cases makes co-operation to achieve global settlements all the more important. She said that '[s]trengthening and deepening the relationships that make this happen is going to be a major focus for me' and listed the newcomer countries to DPAs as part of that focus. Lisa Osofsky, SFO Director, speech at the Cambridge International Symposium on Economic Crime 2018, Jesus College, Cambridge, 3 September 2018, available at www.sfo.gov.uk/2018/09/03/lisa-osofsky-making-the-uk-a-high-risk-country-for-fraud-bribery-and-corruption/. A year on, co-operation continues to be central to the SFO's strategy: 'The work we at the SFO have been able to do in the last year with our international law enforcement partners has been energising – at times even inspiring. Prosecutors all around the world are realising how much we need each other if we are truly to do justice. So we are increasingly linking arms in the march against transnational fraud and corruption.' Lisa Osofsky, 2 September 2019, available at https://www.sfo.gov.uk/2019/09/02/cambridge-symposium-2019/.

the company as a whole.[3] Key benefits of self-reporting include the ability to manage the timing and content of the information being provided to the authorities, the potential for securing a DPA (or other negotiated settlement), reducing any financial penalties, minimising or managing reputational fallout, and achieving an earlier and more predictable resolution than may otherwise be possible. Particular risks include potential disruptive and damaging action by investigating authorities, damage to share prices, the removal or suspension of senior management,[4] costly internal investigations (including potential regulator involvement and the potential loss or waiver of privilege over key material) and potential civil litigation. The still relatively small body of decided cases in relation to DPAs, together with guidance setting out the circumstances in which they will be contemplated and entered into, provide some direction as to whether self-reporting may produce a negotiated outcome.

The stakes for individuals (usually directors) are also higher than ever in the United Kingdom – those working in firms regulated by the Financial Conduct Authority (FCA) or the Prudential Regulation Authority (PRA) will need to consider how the (relatively) new individual accountability regimes may provide those regulators with an easier route to regulatory enforcement action against them, in addition to any criminal and civil liability.

Frequently, questions as to how to deal with internal disclosures made by whistleblowers and, in those circumstances, whether, when and how to self-report matters to authorities, go hand in hand. Similarly, where a corporate operates in multiple jurisdictions, any trigger of mandatory reporting obligations in one jurisdiction warrants careful consideration regarding corresponding mandatory or voluntary reporting in others – particularly in light of authorities' increasingly collaborative approach to (formal and informal) sharing of information.[5]

The decisive and effective management of the risks and benefits of self-reporting, which typically involves balancing complex questions of fact and (criminal, regulatory and employment) law is critical and can help to conclude swiftly or pre-empt regulatory intervention. All these considerations play out against the backdrop of an obvious tension between self-reporting with sufficient speed to obtain or maximise co-operation credit and the chance of a DPA on the one hand, and taking

3 Companies Act 2006, s.172.

4 Alun Milford, then General Counsel at the SFO, said in a speech in September 2017 that in all DPA judgments to date, a key element has been the extent of reform in the corporate, including the removal of senior managers who were either implicated in, or should have been aware of, the criminality concerned, available at www.sfo.gov.uk/2017/09/05/alun-milford-on-deferred-prosecution-agreements/.

5 For example, in its recently published Corporate Co-operation Guidance, the SFO has set out certain indicators of good practice that they would expect to see in a co-operating corporate, including that an organisation should '[n]otify the SFO of any other government agencies, domestic or foreign, law enforcement or regulatory) by whom the organisation has been contacted or to whom it has reported', SFO Operational Handbook, Corporate Co-operation Guidance, p. 4, available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

the time to investigate an allegation sufficiently to understand whether, when and what to report on the other. The Court of Appeal's 2018 decision in the *ENRC* case[6] emphasises the importance (for the purposes of asserting legal privilege) of recording clearly and in good time the points at which a firm considers that it is involved in the self-reporting process and that litigation or criminal prosecution is reasonably in contemplation.

This chapter examines how authorities are using and interpreting self-reporting and whistleblowing frameworks in the United Kingdom, and identifies key considerations for corporates and their advisers. The extraterritorial reach of several pieces of key legislation (most notably the Bribery Act 2010 (UKBA)) and the comparatively aggressive stance of UK investigating and prosecuting authorities (principally the Serious Fraud Office (SFO)) mean that developments in the country are of interest to corporates operating around Europe and the Middle East, even if they are based, or undertake most of their activities, outside the United Kingdom.

3.2 Culture and whistleblowing

3.2.1 The importance of culture

Self-reporting and whistleblowing are increasingly considered to be fundamental to the 'culture' of an organisation. In the wake of the financial crisis and well-publicised corporate scandals, UK regulators and enforcement authorities remain concerned with promoting cultural change across financial institutions and corporates. Particular emphasis is placed on the need for meaningful challenge by (and of) senior management in addition to appropriately robust whistleblowing procedures, which employees are expected to use without fear of reprisal.

The FCA Handbook and PRA Rulebook set out the authorities' expectations that regulated firms will consider adopting internal procedures encouraging workers to blow the whistle internally about matters relevant to the functions of the FCA or PRA.[7] What is more, in response to recommendations by the Parliamentary Commission on Banking Standards in 2013, the FCA and the PRA published new rules, which have made it a requirement (since 7 March 2017) for in-scope banks and insurance firms to allocate responsibility for whistleblowing under the individual accountability regimes (i.e., the Senior Managers Regime, and the Senior Insurance Managers Regime) to a 'whistleblowers' champion', who must be a non-executive director.[8]

6 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corp. Ltd* (ENRC) [2018] EWCA Civ 2006.

7 FCA Handbook, SYSC 18.2.2 G.

8 FCA Policy Statement PS15/24 containing the FCA rules applicable to deposit takers with assets over £250 million. The rules are set out in the FCA Handbook at SYSC 18.1, SYSC 18.31, and SYSC 18.4 and 18.5. The PRA rules are set out in its Policy Statement PS24/15, the PRA General Organisational Requirements Rulebook (applicable to CRR firms, i.e, UK banks, building societies or investment firms subject to the EU Capital Requirements Regulation No. 575/2013) and its Whistleblowing Rulebook (applicable to solvency II firms) and PRA Supervisory Statement

Versions of these individual accountability rules are being introduced for all UK-regulated financial services firms. At the time of writing, the rules giving effect to this extension were due to enter into force in December 2019. There are variations as to how, and the extent to which, some aspects of the regulators' rules and guidance on whistleblowing apply to different types of financial services firms. However, regulatory guidance makes clear that other types of firms should regard the stringent rules currently in place for banks and insurers as best practice and that failures to implement appropriate arrangements may have adverse consequences on the assessment of firms' and individuals' ability to meet the required threshold conditions and fitness and propriety standards.[9]

In firms where one is required, the whistleblowers' champion is responsible for overseeing the effectiveness of internal whistleblowing procedures, including arrangements for protecting whistleblowers against detrimental treatment, preparing an annual report to the board, and reporting to the FCA where, in a case contested by the firm, an employment tribunal finds in favour of a whistleblower. Selection of the whistleblowers' champion should involve careful consideration of the proposed individual's standing and role within the firm, as well as the capacity, resources and access (e.g., to people and information) necessary to effectively discharge the responsibility for 'ensuring and overseeing the integrity, independence and effectiveness of the firm's policies and procedures on whistleblowing and for ensuring staff who raise concerns are protected from detrimental treatment'.[10] As a result of this new whistleblowing regime, the significance of whistleblowers will likely only increase.

Whistleblowing also features in the UKBA framework – under section 7 of the UKBA, a relevant corporate organisation commits an offence where a person associated with it bribes another person, intending to obtain or retain business or a business advantage for the firm. The firm has a defence if it can show that it had in place 'adequate procedures' to prevent such bribery. The Ministry of Justice published statutory guidance on 'adequate procedures' in March 2011, pursuant to section 9 of the UKBA.[11] That guidance recommends that adequate procedures should include procedures for reporting bribery 'including "speak up" or "whistleblowing" procedures'.[12]

SS 39/15 (applicable to deposit takers with assets greater than US$250 million, PRA designated investment firms and insurers).

9 FCA Handbook, SYSC 18.1.1AA G, 18.1.1C G and 18.3.9 G.

10 FCA Handbook, SYSC 18.4.4.R.

11 Ministry of Justice 'Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing', available at www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf, March 2011.

12 Ibid. at para. 1.7. See also *SFO v Tesco Stores Limited* (2017) (Case No. U20170287) [2019] Lloyd's Rep FC 283, Approved Judgment, para. 60(ii), in which Leveson P set out the 'tangible remedial measures, that can properly be described as wide-ranging and comprehensive' and that included the relaunch of Tesco's 'externally-run whistle-blowing service, which is promoted to colleagues and suppliers, so as to raise awareness'.

Similarly, whistleblowing is featured in guidance published by the UK tax authority, HM Revenue and Customs (HMRC), in February 2019 in relation to the corporate offences of failing to prevent the facilitation of tax evasion under sections 45 and 46 of the Criminal Finances Act 2017 (CFA). It is a defence to those offences to show that 'reasonable prevention procedures' were in place (or that it was reasonable not to have any in place). Although, like its equivalent issued in respect of the UKBA, it is careful to avoid prescribing which particular measures specific corporate entities should have in place, the guidance issued by HMRC indicates that a demonstrable commitment to whistleblowing may assist corporate entities with establishing that arrangements maintained by them amounted to 'reasonable prevention procedures'.

Codes that govern prosecutors' decisions to bring charges against corporates,[13] and the DPA Code of Practice (the DPA Code)[14] itself, set out public interest factors for and against prosecution,[15] which, as Lisa Osofsky put it recently, 'instruct us to take into account the existence of effective compliance programmes and speedy self-reporting. It is about incentivising the private sector to cooperate in preventing crime, to be willing to report it if it occurs nonetheless, and to cooperate when we investigate and prosecute those who have transgressed.'[16] A self-report is also relevant at later stages in the UK criminal justice process. The Sentencing Council's Definitive Guideline,[17] which was effective from 1 October 2014 in relation to the sentencing of corporates for fraud, bribery and money laundering offences, and which is considered in setting financial penalties under a DPA, takes into account a corporate's culture in the event of a conviction.[18] Further, the amended Public Contracts Regulations 2015, introduced in February 2015, allow blacklisted companies to bid for public contracts if they can prove (among other things) that they have 'clarified the facts and circumstances in a comprehensive manner by actively collaborating with the investigating authorities' and 'taken concrete technical, organisational and personnel measures that are appropriate to prevent further criminal offences or misconduct'.[19]

13 https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/corporate-self-reporting/.

14 Deferred Prosecution Agreement Code of Practice issued by the Director of Public Prosecutions and Director of the SFO pursuant to the Crime and Courts Act 2013, available at www.cps.gov.uk/sites/default/files/documents/publications/dpa_cop.pdf.

15 DPA Code, s.2.

16 Lisa Osofsky, SFO Director, speech at the Cambridge International Symposium on Economic Crime 2019, Jesus College, Cambridge, 2 September 2019, available at https://www.sfo.gov.uk/2019/09/02/cambridge-symposium-2019/.

17 Sentencing Council's Definitive Guideline 'Corporate Offenders: Fraud, Bribery and Money Laundering', available at www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-bribery-and-money-laundering-offences-Definitive-guideline2.pdf.

18 A culture of wilful disregard for the commission of offences will lead to a corporate being placed at the most culpable end of the spectrum and facing the heaviest fines available.

19 The Public Contracts Regulations 2015, Regulation 57(15).

Whistleblowing 3.2.2

The SFO launched its whistleblowing hotline (SFO Confidential) in 2011, although reports are now made electronically to the SFO's Intelligence Unit through the 'secure reporting form'.[20] The SFO's take-up of cases for investigation, based on such reports, remains low.[21]

The FCA managed 1,119 cases from whistleblowers in 2018, taking further action in 95 of these. The FCA has previously indicated that it expects to see an increase in the proportion of reports that lead directly to enforcement action or other intervention, or that provide intelligence of significant value, although these predictions are yet to come to fruition as the proportion of cases in which it has taken action has in fact declined slightly in recent years (10 per cent in 2017 and 8.5 per cent in 2018).[22]

The SFO has been keen to emphasise that whistleblowing is one avenue by which it may come to hear of alleged criminal conduct: 'Any such source can give us, or more particularly the Director, reasonable grounds to suspect the commission of an offence involving serious fraud, bribery or corruption and, with it, the power to open a criminal investigation.'[23] However, while whistleblower reports in the United Kingdom account for a proportion of the investigations commenced by the SFO, they are by no means the majority. They have led to some relatively high-profile successful prosecutions, although to date these have largely concerned individuals rather than corporate organisations.[24] More are expected to follow, including some of the SFO's current flagship investigations and prosecutions into large corporates. In September 2013, the SFO commenced criminal proceedings against Gyrus Group Limited, the UK subsidiary of Olympus Corporation, in connection with a worldwide fraud valued at approximately US$1.7 billion. That investigation flowed from the widely publicised whistleblowing disclosure made by Michael Woodford, the former CEO of Olympus, although the investigation has since been discontinued following a Court of Appeal judgment in February 2015, which ruled that English law does not criminalise the misleading of auditors by the company under audit. Separately, in December 2012, the SFO started an investigation into Rolls-Royce plc following a whistleblower report, although, despite the company having concluded a DPA with the SFO in

20 The secure reporting form is available at https://www.sfo.gov.uk/contact-us/reporting-serious-fraud-bribery-corruption/.

21 Number of SFO Investigations, July 2019, available at https://www.sfo.gov.uk/publications/corporate-information/freedom-of-information/.

22 See www.fca.org.uk/static/documents/how-we-handle-disclosures-from-whistleblowers.pdf.

23 Alun Milford, then General Counsel at the SFO, speech at the Cambridge Symposium on Economic Crime 2014, Jesus College, Cambridge ('The Use of Information to Discern and Control Risk'), 2 September 2014, available at www.sfo.gov.uk/2014/09/02/alun-milford-use-information-discern-control-risk/.

24 See, for example, prosecutions of individuals associated with Torex Retail PLC: https://www.sfo.gov.uk/2013/06/21/final-conviction-torex-retail-false-accounting-case/.

January 2017,[25] the SFO confirmed in February 2019 that no charges would be brought against individuals. The investigation into ENRC by the SFO was also influenced by whistleblower allegations first made to the company by email and then published in the media a few months later.[26]

See Chapter 19 on whistleblowers

3.3 The evolution of the link between self-reporting and a DPA

DPAs are now an established feature of the UK investigations landscape. The Director of the SFO, Lisa Osofsky, has spoken of her commitment to bringing the most complex and difficult cases of crimes to trial or, if in the public interest, to resolution through DPAs.[27] At the time of writing, five years and five DPAs after the introduction of the regime, there are some useful indications as to the SFO's stance – and equally importantly the courts' – in the cases decided (including those where DPAs have not been concluded), and in the operation of prosecution guidance in ongoing investigations and negotiations that may lead to further DPAs. The SFO's Corporate Co-operation Guidance,[28] issued in August 2019, gives greater clarity about when the SFO will consider a corporate organisation to be behaving sufficiently co-operatively to justify the commencement of discussions about possible negotiated outcomes. The Corporate Co-operation Guidance forms part of the SFO's internal Operational Handbook. It is published on the SFO's website in the interests of transparency, and the Guidance clearly states that it does not create legally enforceable rights, expectations or liabilities. The Guidance sets out what in practice constitutes co-operation. It focuses on the steps companies need to take to assist the SFO with its investigation, including by setting out the SFO's expectations with regard to the timeliness and extent of self-reporting by co-operating corporate organisations; in its introduction, it states:

See Chapter 23 on negotiating global settlements

> *Co-operation means providing assistance to the SFO that goes above and beyond what the law requires. It includes: identifying suspected wrong-doing and criminal conduct together with the people responsible, regardless of their seniority or position in the organisation; reporting this to the SFO within a reasonable time of the suspicions coming to light; and preserving available evidence and providing it promptly in an evidentially sound format.*

However, to understand the effect of any such co-operation, companies and practitioners still have to look to the DPA Code.

---

25 *Serious Fraud Office v. Rolls-Royce plc and Rolls-Royce Energy Systems Inc.* (Case No. U20170036) [2017] Lloyd's Rep FC 249, paras. 21 and 22.

26 *Serious Fraud Office (SFO) v. Eurasian Natural Resources Corp. Ltd* [2018] EWCA Civ 2006, at paras. 16-17.

27 Lisa Osofsky, speech at the Cambridge International Symposium on Economic Crime 2018, Jesus College, Cambridge, 3 September 2018, available at www.sfo.gov.uk/2018/09/03/lisa-osofsky-making-the-uk-a-high-risk-country-for-fraud-bribery-and-corruption/.

28 SFO Operational Handbook, Corporate Co-operation Guidance, p. 1, available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

The DPA Code sets out prosecutors' expectations in relation to self-reporting. A key factor when deciding whether a DPA is appropriate, to be weighed with other factors relating to the nature and seriousness of the offending, is whether the corporate has been 'genuinely proactive' in its approach.[29] This is measured by reference to the factors including the timing of a corporate's self-report, and how comprehensive, relevant and useful the material is (particularly in the context of any potential action to be taken against individuals).

The DPA Code makes clear that the SFO (or Crown Prosecution Service (CPS)) expects to be 'notified' of wrongdoing 'within a reasonable time of the offending conduct coming to light' for a DPA to be a realistic option.[30] The word 'notified' in this context replaced the word 'reported' originally included in the draft of the DPA Code. Although (perhaps given that it was not the subject of a consultation exercise prior to its publication in August 2019) the same distinction between 'reporting' and 'notifying' is not drawn in the Corporate Co-operation Guidance,[31] the message prosecutors are seeking to convey in both the DPA Code and the Corporate Co-operation Guidance is that corporate organisations wishing to obtain as much co-operation credit as possible should not wait until they have carried out their own detailed internal investigation before self-reporting concerns about possible wrongdoing. The Corporate Co-operation Guidance does not provide any further detail about when the SFO expects matters to be brought to its attention. Instead it reiterates previous general indications that this should occur 'within a reasonable time' of the corporate organisation becoming aware of the relevant matters. What is clear is that prosecutors expect to receive an initial notification of circumstances giving rise to concerns that criminal wrongdoing may have occurred. They do not expect or wish to receive a completed investigation report. As is set out in both the Corporate Co-operation Guidance and the DPA Code, they expect to be involved in the investigation at the planning stage and certainly before any witness interviews are conducted.[32] In cases where significant historic wrongdoing that is not already known to prosecutors and may suitably be resolved through a DPA comes to light, firms should consider making an initial notification to the SFO (or CPS, if appropriate) when they file suspicious activity reports (SARs) or other statutory reports (whether in the United Kingdom or abroad).

The timing of notification relative to details entering the public domain is of particular importance. At the time of writing, *Rolls-Royce* remains the highest-value

29 DPA Code, para. 2.8.2.

30 DPA Code, para. 2.8.1(v): 'Failure to notify the wrongdoing within a reasonable time of the offending conduct coming to light.'

31 SFO Operational Handbook, Corporate Co-operation Guidance, at p. 1: 'Co-operation means . . . reporting [suspected wrongdoing] to the SFO within a reasonable time of the suspicions coming to light.', available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

32 DPA Code, para. 2.9.2; SFO Operational Handbook, Corporate Co-operation Guidance, at p. 4: 'To avoid prejudice to the investigation, consult in a timely way with the SFO before interviewing potential witnesses or suspects, taking personnel/HR actions or taking other overt steps.', available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

DPA concluded in the United Kingdom. That it was still possible for the SFO to conclude a DPA with Rolls-Royce in 2017 despite some details of wrongdoing being already known to the SFO illustrates that this is just one factor informing a prosecutor's approach and does not by itself determine whether a DPA will follow.[33] However, as Sir Brian Leveson, then President of the Queen's Bench Division, noted in respect of Rolls-Royce, the case was anomalous in this regard, and it was necessary for the company to provide 'extraordinary' co-operation and to notify the SFO of matters 'of a different order' to those it would otherwise have known to obtain credit for self-reporting in the context of DPA negotiations.[34] Absent such extraordinary co-operation and disclosure, it is clear that a failure to notify the SFO of matters before they become public (or before negative headlines are threatened or imminent) will jeopardise the prospects of successfully negotiating a DPA.

The decision of the SFO in December 2015 to prosecute Sweett Group plc for the corporate offence of failure to prevent bribery under section 7 of the Bribery Act 2010 also illustrates this. Sweett self-reported to the SFO upon learning that a newspaper intended to publish allegations of involvement in bribery in connection with Middle Eastern construction consultancy agreements. Although informal discussions about DPAs did commence at one stage of the SFO's investigation, they were unsuccessful; and Sweett was deemed to have been un-cooperative for much of the investigation, leading ultimately to conviction and the imposition of a fine of £2.25 million in February 2016. Sweett's experience contrasts starkly with that of Standard Bank plc, with which the SFO agreed the first DPA in the United Kingdom in November 2015.[35] The SFO, and subsequently the court, highlighted and commended Standard Bank for reporting concerns to the SFO within weeks of the suspicious payment, and within days of filing a SAR.

The court's judgments in respect of Standard Bank and the other corporates with which DPAs have been concluded have added some colour to the indications in the DPA Code as to what the courts consider a corporate must do in practice when self-reporting to demonstrate 'genuine and proactive' co-operation. As already noted, these indications have been supplemented most recently by the Corporate Co-operation Guidance. Although it reflects what has occurred in previous cases where DPAs have been negotiated and approved (and other decided cases concerning issues arising during SFO investigations) and what continues to happen during discussions between co-operating corporate organisations and the SFO in cases where a DPA may be an option, at the time of writing, it has not been applied or referenced in any reported cases. For now, it has to be read

33 As noted in the Corporate Co-operation Guidance: 'Each case will turn on its own facts. In discussing co-operation with an organisation, the SFO will make clear that the nature and extent of the organisation's co-operation is one of many factors that the SFO will take into consideration when determining an appropriate resolution to its investigation.' Ibid., p. 1.

34 *Serious Fraud Office v. Rolls-Royce plc and Rolls-Royce Energy Systems Inc.* (Case No. U20170036) [2017] Lloyd's Rep FC 249, paras. 21 and 22.

35 *Serious Fraud Office v. Standard Bank plc* (Case No. U20150854) [2016] Lloyd's Rep FC 102.

together with the body of case law relating to DPAs in the United Kingdom. In these cases, 'genuine and proactive' co-operation has manifested itself largely through pragmatic decisions by firms to waive privilege on a limited basis and to make material available voluntarily (i.e., without requiring the SFO to use powers of compulsion, although the Corporate Co-operation Guidance confirms that the fact that the SFO may perceive a need to use its powers of compulsion will not necessarily mean that the corporate organisation concerned is not behaving suitably co-operatively). In all cases it has been crucial to show clear separation from the individuals alleged to have been involved in wrongdoing and commitment to providing material to be used in prosecutions against them, although in no case yet concluded has such material contributed to the conviction of any individual for the conduct in respect of which the corporate entity entered into a DPA.[36]

In early 2018, the CPS sent a useful reminder that self-reporting, however promptly, is only one factor influencing whether a DPA may be available. In *R v. Skansen Interiors Ltd*[37] – the first contested case in relation to the corporate 'failure to prevent' offence under section 7 of the UKBA – Skansen was prosecuted despite self-reporting to the National Crime Agency (NCA) and provided extensive co-operation to the CPS in the ensuing criminal investigation, including by disclosing privileged material. Skansen argued in court that its policies and procedures were adequate for a small company with operations only in the United Kingdom and a staff of 30, but the jury returned a guilty verdict, finding that the policies and procedures in place were insufficient for the purposes of the 'adequate procedures' defence. The CPS justified its decision to prosecute rather than pursue a DPA on grounds that Skansen was a dormant company and could neither pay a fine nor comply with the terms of any DPA, and that it wanted to send a message more generally to smaller companies as regards the importance of having effective anti-bribery and corruption procedures in place, rather than relying on 'company values' to establish proper compliance and conduct.

Key self-reporting requirements in the United Kingdom 3.4

Considerations for reporting may broadly be broken down into two categories – matters firms must report under legislation or regulation, and matters they may choose to report in the hope of bringing about an earlier or more favourable resolution to an investigation. These are examined separately below.

36 The most recent examples are the discontinuation of proceedings against former senior executives of Tesco Stores Limited in late 2018 (https://www.sfo.gov.uk/2018/12/06/no-case-to-answer-ruling-in-case-against-former-tesco-executives/) and the acquittal in July 2019 of employees of Sarclad Limited (which was anonymised as 'XYZ' when the DPA was entered into with the company, at which point reporting restrictions were in place due to the continuing proceedings against three employees (https://www.sfo.gov.uk/2019/07/16/three-individuals-acquitted-as-sfo-confirms-dpa-with-sarclad/)).

37 *R v. Skansen Interiors Limited*, unreported.

3.4.1 Anti-money laundering and terrorist financing reporting obligations

The sections of the United Kingdom's anti-money laundering and counter-terrorist financing legislation dealing with reporting are among the most stringent of their type in the world.

In outline, the Proceeds of Crime Act 2002 imposes specific obligations on businesses operating in the 'regulated sector' to make SARs to the NCA where they know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.[38]

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLTF Regulations) require firms that are 'relevant persons'[39] to appoint a nominated officer and to ensure that anyone who is working in the firm, handling relevant business and has the requisite suspicion in relation to money laundering will make an internal report to the nominated officer, who is then obliged to consider whether to file a SAR.[40] This means that there are (internal) reporting obligations on the individuals working in those firms. For businesses operating in the regulated sector, information triggering reporting obligations is likely to have come to them as a consequence of customer due diligence and monitoring obligations imposed by the Money Laundering Regulations 2007 and the MLTF Regulations.

SARs may include a request to the NCA for 'appropriate consent' to enable the reporter to do a particular act in relation to the property concerned, which might otherwise amount to the commission of a money laundering offence.[41] Such SARs have historically been referred to as 'consent SARs', although they are now referred to by the NCA as 'requests for a defence against money laundering' or 'DAML SARs'.

There is a corresponding reporting and consent regime in relation to terrorist financing under the Terrorism Act 2000.[42] In addition, authorities may impose specific obligations on financial institutions, in particular, to report dealings with certain 'designated persons'.[43]

The relatively low threshold for making a SAR and the natural desire of businesses and the individuals within them to avoid liability (which can include potentially lengthy periods of imprisonment for individuals) means the NCA receives very substantial volumes of DAML SARs, placing a significant strain on its resources. In a review of the SAR framework completed in July 2018, the Law Commission acknowledged this, identifying that, on average, the relevant section

38 The Proceeds of Crime Act (POCA), ss.330 and 331.

39 A firm will be a 'relevant person' if it falls within the MLTF Regulations' definitions of: (1) credit institutions; (2) financial institutions; (3) auditors, insolvency practitioners, external accountants and tax advisers; (4) independent legal professionals; (5) trust or company service providers; (6) estate agents; (7) high value dealers; (8) casinos. (MLTF Regulations, regulation 8).

40 MLTF Regulations, regulations 19 and 20.

41 POCA, ss.335 and 336.

42 The Terrorism Act 2000 (TACT), s.21A (duty for the regulated sector), s.19 (duty outside the regulated sector) and s.21ZA (consent).

43 Counter-Terrorism Act 2008, Schedule 7, para. 12, and Terrorist Asset Freezing Act 2010, s.19.

of the NCA receives 2,000 SARs per working day, with some 100 reports seeking consent to proceed with a financial transaction.[44]

The number of SARs submitted remains high: the most recent statistics released by the NCA indicate that 478,437 SARs were filed between April 2018 and March 2019 (of which 34,151 were DAML SARs).[45] The statistics also show that the number of staff within the relevant section of the NCA is increasing (to 115 at the time of writing).

However, for the time being at least, the volume of SARs, together with the need for the NCA to consult with other enforcement authorities potentially interested in the information (of which there will be many), typically means that the NCA is not in a position to provide consent, or to confirm whether the reporter has 'appropriate consent' to proceed (in NCA parlance, whether the reporter has a 'defence against money laundering') much before the end of the seven-working-day notice period following the filing of a SAR.[46] This can lead to practical problems during the notice period itself and, if applicable, during the following moratorium period (which may now be extended to up to six months on the application of investigating authorities). Transactions will not be able to proceed. The risk of tipping off or committing other offences also leads to difficulties when communicating with customers, counterparties and others. The courts have been reluctant to interfere to accelerate this process.[47]

The Law Commission's review of the effectiveness of the United Kingdom's suspicious activity reporting regime for money laundering has acknowledged that more changes to existing frameworks are required. It has proposed changes including further practical guidance on key tenets of the reporting regime, such as the meaning of 'suspicion', but has stopped short of recommending other more radical changes originally mooted, such as amending the threshold for reporting matters to the NCA.[48]

In practice, a firm's decision whether and when to file SARs to comply with reporting obligations or to secure defences to substantive offences must form one part of wider strategic calculations about self-reporting. In many cases, it will be clear which enforcement authorities will be interested in investigating the circumstances that have given rise to knowledge or suspicion of (or reasonable grounds to suspect) money laundering. In such cases, it can make sense to consider providing

44 Law Commission's Consultation Paper, July 2018.

45 POCA, ss.335 (appropriate consent) and 336 (nominated officer consent). The NCA's most recent statistics indicate that the average turnaround time for a DAML SAR is five to 12 days. See the NCA's annual SAR report, November 2019, available at https://nationalcrimeagency.gov.uk/who-we-are/publications/390-sars-annual-report-2019/file.

46 The NCA's most recent statistics indicate that the power to extend the moratorium period was used 70 times in 2018–2019. See the NCA's annual SAR report, November 2019, available at https://nationalcrimeagency.gov.uk/who-we-are/publications/390-sars-annual-report-2019/file.

47 See *National Crime Agency v. N* [2017] EWCA Civ 253; and *Lonsdale v. Natwest* [2018] EWHC 1843 (QB), for example.

48 Law Commission, 'Anti-Money Laundering: The SARs Regime Report', Law Com No. 384 (June 2019), available at https://www.lawcom.gov.uk/project/anti-money-laundering/.

the information set out in the SAR to the relevant enforcement authorities. Doing so when filing a SAR with the NCA (or soon after) can help to secure maximum credit for proactively bringing matters to the attention of the authorities and to expedite obtaining consent to proceed with a transaction.

3.4.2 Other mandatory reporting obligations prescribed by legislation

A company will be subject to a variety of reporting obligations, depending on the nature of its operations, the sector in which it is involved, and the extent (and by which authorities) it is regulated. Each authority will have its own requirements as to the timing, format, content and process for mandatory reports. The key sectoral requirements include reporting:

- financial sanctions breaches, to the Office for Financial Sanctions Implementation (OFSI) (on behalf of Her Majesty's Treasury);
- (for financial institutions) the corporate offences of failure to prevent the facilitation of UK or foreign tax evasion under the CFA to HMRC;[49] and
- data security breaches under the General Data Protection Regulation (GDPR), within 72 hours of becoming aware of the breach, to the Information Commissioner's Office (ICO) and, in some cases, to the data subjects concerned.

3.4.3 Self-reporting obligations in DPAs and regulatory and private agreements

Separately, corporates may have self-imposed reporting obligations. It is common for certain reporting obligations to be built into DPAs, ongoing monitorship agreements or other agreements with regulators in relation to historic criminal or regulatory failings, for example. Where a firm has a history of such failings, it is also not uncommon for parties to key transactional and financial agreements to insist on similar reporting obligations, often tied to the corporate's mandatory reporting requirements to particular authorities. In all cases, these obligations may have short reporting windows, which should be familiar to the corporate and acted on without undue delay.

Separately, corporates may be obliged to bring the fact of an investigation, or the circumstances giving rise to it, to the attention of a host of potentially interested parties. These may include regulators, contractual counterparties, markets on which they are listed, affected customers and insurers. There is a relatively high likelihood of variations in contractual arrangements and legal and regulatory frameworks (for example, in relation to conditions for contracting with government entities under applicable public procurement legislation) across the jurisdictions in which corporates operate. Conducting an early analysis of the potential

49 The term 'corporate offences' refers to the 'failure to prevent the facilitation of tax evasion' offences created by s.45 (in relation to UK tax) and s.46 (in relation to foreign tax) of the Criminal Finances Act 2017, pursuant to which a financial institution must report on any failure to prevent the criminal acts of its employees and other associated persons who have intentionally facilitated tax evasion while providing a service for it or on its behalf.

collateral impact of historic wrongdoing and any investigation, prosecution or negotiated outcome, will therefore often be prudent.

Self-reporting to the FCA and PRA 3.4.4

The FCA and, in the case of dual-regulated firms, the PRA are responsible for the conduct of firms authorised under the Financial Services and Markets Act 2000. Of particular relevance is the responsibility for ensuring that the firms and individuals regulated by it establish and maintain effective, proportionate and risk-based systems and controls to ensure that they cannot be used for the purposes of financial crime.[50]

The FCA Handbook and the PRA Rulebook contain detailed rules and guidance on its requirements in this area. These provisions supplement the overarching obligations on regulated firms and individuals to maintain an 'open and co-operative' relationship with the FCA and PRA and to 'disclose . . . appropriately anything relating to the firm of which [the relevant regulator] would reasonably expect notice'.[51] In practice, these broad principles-based requirements oblige regulated firms and individuals to notify the FCA or the PRA, or both, not only of circumstances that may amount to breaches of rules set out in the FCA Handbook or the PRA Rulebook, but also of investigations and other matters that may affect the fitness and propriety of individuals, or the ability of firms to satisfy the threshold conditions required to be authorised to carry on particular regulated activities.

In recent years, the FCA has increasingly used its enforcement powers against firms and individuals for deficiencies in financial crime systems and controls. It continues to do so enthusiastically, with the most recent statistics published by the FCA indicating that it has approximately 88 such investigations open at the time of writing. It looks set to continue in this vein, having identified the area as one of its 'cross-sector priorities' in its most recent annual report.[52] A number of enforcement cases pursued by the FCA in relation to financial crime systems and controls have been based to a significant degree on failures proactively to bring matters to the FCA's attention.[53] Looking more widely across the FCA's regulatory purview, in a number of other cases substantial penalties have been imposed on firms and individuals simply for failing to comply with obligations to notify the regulator.[54]

50 See the FCA's Annual Report for 2018/19, available at https://www.fca.org.uk/annual-report-and-accounts-2018-19.

51 PRIN 2.1.1 R, Principle 11 of the Principles for Businesses (Relations with Regulators).

52 FCA Enforcement annual performance report 2018/19, available at https://www.fca.org.uk/publication/corporate/annual-report-2018-19-enforcement-performance.pdf.

53 For example, in 2015 the FCA fined The Bank of Beirut (UK) Ltd (Bank of Beirut) £2.1 million, prevented it from acquiring new customers from high-risk jurisdictions for 126 days, and fined two approved persons at the bank. The FCA noted that Bank of Beirut had also repeatedly provided the FCA with misleading information after it was required to address concerns regarding its financial crime systems and controls, including by indicating that it had completed remedial actions when it had not.

54 For example, in 2018, Santander was fined for, among other things, failing to disclose information relating to certain issues with the probate and bereavement process to the FCA. The final notice

In a number of other areas, firms and individuals must proactively bring particular matters to the attention of the FCA, which may in due course give rise to intensified supervision, or enforcement investigations, or both. Key examples include obligations to file suspicious transaction and order reports under the Market Abuse Regulation and requirements for firms to notify the FCA (or PRA, as appropriate) of breaches of the Conduct Rules by senior managers, certified persons or other employees. The timescales for such notifications and the level of detail required also vary significantly depending on the circumstances.

The FCA also acts as the UK Listing Authority, meaning that companies listed in the United Kingdom (and their directors) must behave in an open and co-operative manner.[55] Although the wording of the requirement imposed on listed companies differs from that imposed on regulated firms and individuals (it does not include an express requirement to notify the FCA of matters of which it would reasonably expect notice), listed companies and their directors should expect to have to notify the FCA of potentially significant investigations under these obligations.

None of the mandatory reporting obligations described above exists in a vacuum. The FCA in particular collaborates closely with other enforcement authorities within the United Kingdom and internationally.

Indeed, notwithstanding its ability to prosecute criminal offences, there have been several examples in recent years of cases in which it has supplied information to and otherwise coordinated its action with other authorities, including, notably, the SFO.[56]

The remainder of this chapter considers self-reporting in relation to the SFO and, to the extent relevant, the FCA, in relation to financial crime issues.

3.5 Voluntary self-reporting to the SFO

The SFO's decision as to whether to prosecute a corporate organisation will be governed by a combination of the 'Full Code Test' in the Code for Crown Prosecutors,[57] the Guidance on Corporate Prosecutions,[58] (in relevant cases) the

is available at https://www.fca.org.uk/publication/final-notices/santander-uk-plc-2018.pdf. In June 2019, the FCA fined Bank of Scotland £45.5 million for failing to disclose suspicions that fraud may have taken place within part of its corporate lending operations. The final notice is available at https://www.fca.org.uk/publication/final-notices/bank-of-scotland-2019.pdf.

55 FCA Handbook, LR 7.2.1 R, Listing Principle 2.

56 By way of recent example, the FCA did not impose a financial penalty on Tesco plc or Tesco Stores in early 2017 for engaging in market abuse, partly because Tesco Stores had entered into a DPA with the SFO, pursuant to which it would pay £128.9925 million. The FCA explained that it had also taken into account 'the exemplary co-operative approach' taken by Tesco plc and Tesco Stores with both the FCA and the SFO. See the FCA final notice, available at www.fca.org.uk/publication/final-notices/tesco-2017.pdf.

57 The Code for Crown Prosecutors, available at www.cps.gov.uk/publication/code-crown-prosecutors.

58 The joint guidance issued by the Director of Public Prosecutions, the Director of the Serious Fraud Office and the Director of the Revenue and Customs Prosecutions Office Guidance on Corporate Prosecutions, available at www.sfo.gov.uk/?wpdmdl=1457.

Joint Prosecution Guidance of the Director of the SFO and the Director of Public Prosecutions on the Bribery Act 2010 (the Joint UKBA Guidance), the DPA Code of Practice and the Corporate Co-operation Guidance.[59]

The SFO will prosecute if there is a realistic prospect of conviction on the evidence, and it is in the public interest to do so. The fact that a corporate has reported itself will be a relevant consideration to the extent set out in the Guidance on Corporate Prosecutions. That guidance explains that, for a self-report to be a public interest factor tending against prosecution, it must form part of a 'genuinely proactive approach adopted by the corporate management team when the offending is brought to their notice'.[60] The SFO has long stated expressly, and has reiterated most recently in the Corporate Co-operation Guidance, that self-reporting is no guarantee that a prosecution will not follow, and that each case will turn on its own facts.[61]

The Corporate Co-operation Guidance 'does not seek to set out exhaustively what will be required in order for a corporate organisation to be considered as genuinely co-operative and indeed is clear that there will be dialogue in every case about what will be expected of the corporate organisation concerned'. It does add detail and confirm previous public statements in relation to some practical steps corporate organisations should take, including good general practices surrounding the preservation and production of relevant digital and hard copy information; good practice concerning evidence of financial records and analysis (to 'show relevant money flows'); the provision of industry and background information (including about other actors in the market and whether any other government agencies are aware); and good practice concerning taking witness evidence (including an expectation that co-operating corporates will waive privilege over witness accounts).

In appropriate cases the SFO may use its powers under proceeds of crime legislation as an alternative (or in addition) to prosecution.[62] If the SFO uses those powers, it will publish its reasons, the details of the illegal conduct and the details of the disposal.

Advantages of self-reporting 3.5.1

Co-operation credit 3.5.1.1

Most corporates will consider that the primary advantage of making a voluntary self-report is co-operation credit, particularly if the corporate is seeking a DPA. Speaking in June 2018, Camilla de Silva, the SFO's Joint Head of Bribery and

59 Bribery Act 2010: Joint Prosecution Guidance of The Director of the Serious Fraud Office and The Director of Public Prosecutions, 30 March 2011, available at www.sfo.gov.uk/?wpdmdl=1456.

60 Guidance on Corporate Prosecutions, para. 32 ('Additional public interest factors against prosecution').

61 SFO's statement of policy and revised guidance on corporate self-reporting, October 2012.

62 See the Attorney General's Guidance for prosecutors and investigators on their asset recovery powers under s.2A POCA, available at www.gov.uk/guidance/asset-recovery-powers-for-prosecutors-guidance-and-background-note-2009.

Corruption, said: 'The SFO will only invite a company to enter into an agreement to defer prosecution where the company has genuinely co-operated with the SFO.'[63] This statement reflects the DPA Code, which lists co-operation as an additional public interest factor tending against prosecution.[64] As noted earlier, the DPA Code is clear that the co-operation has to be 'genuinely proactive' and lists as examples of co-operative behaviour 'identifying relevant witnesses, disclosing their accounts and the documents shown to them . . . [and] where practicable it will involve making the witnesses available for interview when requested'.[65]

The Guidance on Corporate Prosecutions also lists co-operation as a factor tending against prosecution, but instructs prosecutors to 'establish whether sufficient information about the operation of the company in its entirety has been supplied in order to assess whether the company has been proactively compliant' before taking co-operation into account as a factor, and stresses that '[t]his will include making witnesses available and disclosure of the details of any internal investigation'.[66]

In approving DPAs between the SFO and each of Standard Bank, Sarclad Ltd,[67] (which in the initial preliminary and approved judgments had been identified as XYZ Ltd) and Rolls-Royce, Sir Brian Leveson, then President of the Queen's Bench Division, spoke approvingly of the co-operative stance adopted by each of those firms, as did Mr Justice William Davis, approving the DPA between the SFO and Serco Geografix Limited in July 2019.[68]

Even if a corporate reports at an early stage and takes every step to co-operate with the SFO, it may still not be considered eligible for a DPA because other factors ward against it, for example where the behaviour in question has caused a significant level of harm to victims, or a substantial adverse impact to the integrity or confidence of markets.[69]

Following conviction or a guilty plea, a corporate is still likely to receive some benefit from its co-operation when it comes to sentencing. The Sentencing Council's Definitive Guideline sets out a multi-step process to assist courts in determining the appropriate fine. The first step is to establish the harm caused by the offending. For example, for a bribery offence, the starting point for the calculation is the 'harm figure' – the gross profit from the contract obtained. Once a harm figure has been determined, the court has to establish the 'culpability' factor by reference to a scale in the Definitive Guideline (from 'A' for high culpability down to 'C' for lesser culpability). Each level of culpability has attached to it a

63 Camilla de Silva, SFO Joint Head of Bribery and Corruption, speech at the Herbert Smith Freehills Corporate Crime Conference 2018, available at www.sfo.gov.uk/2018/06/21/corporate-criminal-liability-ai-and-dpas/.

64 Para. 2.8.2(i).

65 Ibid.

66 Guidance on Corporate Prosecutions, p. 8.

67 *Serious Fraud Office v. XYZ Limited* (Case No. U20150856) [2016] 7 WLUK 220; [2016] Lloyd's Rep FC 509.

68 *Serious Fraud Office v. Serco Geografix Ltd* [2019] (Case No. U20190413) 7 WLUK 45.

69 DPA Code, para 2.8.1(vii).

range of multipliers to apply to the harm figure. In determining exactly which multiplier to apply, the court must take into account many factors. Notably, co-operation with the investigation is listed in the Definitive Guideline as a factor that will tend to reduce the culpability multiplier.

Arguably, corporates in the regulated sector have less scope for truly voluntary self-reporting because the requirement in Principle 11 of the FCA's Principles for Businesses require a regulated firm to 'disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice'.[70] The FCA sets out in its Decision Procedure and Penalties Manual (DEPP) a non-exhaustive list of factors it will consider when deciding to issue a financial penalty or public censure. Included on the list of factors is 'how quickly, effectively and completely the person brought the breach to the attention of the FCA or another relevant regulatory authority'.[71] If the FCA does choose to take action against a firm, DEPP includes provisions for determining the appropriate level of financial penalty, which operate similarly to the Sentencing Council's Definitive Guideline. DEPP states that a factor to consider when deciding whether to increase or decrease any fine is 'the conduct of the firm in bringing (or failing to bring) quickly, effectively and completely the breach to the FCA's attention'.[72]

Demonstrating culture and the strength of systems and controls 3.5.1.2

Effective self-reporting will clearly indicate a good corporate culture. Firms that have taken the necessary steps to institute a good culture supported by robust systems and controls will expect that any matters involving wrongdoing are quickly reported internally via its whistleblowing procedures and escalated and reported to the relevant authorities, as appropriate.

Conversely, for firms in the regulated sector, the failure to identify and self-report wrongdoing could indicate that its systems and controls are inadequate. The FCA Handbook states that a regulated firm:

> *must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime.*[73]

There are a number of examples of the FCA taking enforcement action in recent years against regulated firms for having inadequate systems and controls.[74]

70 FCA Handbook, PRIN 2.1.1 R. An equivalent obligation to notify the PRA is set out in Fundamental Rule 7.

71 FCA Handbook, DEPP 6.2.1 (2)(a).

72 FCA Handbook, DEPP 6.5A.3 (2)(a).

73 FCA Handbook, SYSC 6.1.1R.

74 For example, the FCA's fine of Bank of Beirut, discussed above.

In a slightly different context, a recently concluded case concerning whether the actions of an investment bank in paying away monies held in the account of a company to its director amounted to negligence highlights the potentially substantial losses that may result from inadequacies in systems and controls, even if no regulatory or criminal enforcement action is taken against the institution concerned.[75]

3.5.1.3 Information control

Firms often think that choosing to self-report will enable them to retain control over the information that they disclose. In practice, however, the SFO and FCA's insistence on effective and complete self-reporting means that firms will have to provide as complete an account as possible of the wrongdoing concerned, and hand over any investigative work-product already created. Public companies will also have to give careful consideration to their obligations to make market announcements.

See Chapter 37 on publicity and Chapter 39 on protecting corporate reputation

Given the stance adopted by the FCA and SFO, perhaps the only true benefit to self-reporting is that the corporate has some control over the timetable (as compared, for instance, with a dawn raid) and is therefore able (having taken advice on any market abuse risks) to notify key stakeholders of the self-report and to prepare an appropriate media strategy.

3.5.2 Risks of self-reporting

For many companies, the primary driver behind self-reporting is the opportunity to secure a DPA. It should be clear from the analysis above, however, that self-reporting in the United Kingdom does not guarantee a DPA or even necessarily leniency in sentencing (depending on whether other public interest factors are at play). It is also clear that a firm may only be able to gauge its prospects of success relatively late in a process during which the firm will usually have provided a significant amount of information, documents, investigation reports and even witnesses for interview.[76]

Perversely, therefore, a firm's efforts to secure maximum co-operation credit may actually put it in a worse position than it began in, especially if it has provided information or evidence about an issue or facts that may not otherwise have come to light or been obtainable by the authority. There is an ever-present risk that by the time the corporate has visibility as to the direction in which the SFO or the court is leaning, it may have assisted prosecutors in building a strong case against itself, often at significant financial and other cost, for little or no benefit. The Corporate Co-operation Guidance provides the most recent reminder of this, with clear express warnings to corporate organisations that none of its provisions creates any rights or expectations. In a slightly different context, *Soma Oil*

75 *Singularis Holdings Ltd (In Official Liquidation) (A Company Incorporated in the Cayman Islands) v. Daiwa Capital Markets Europe Limited* [2019] UKSC 50.

76 In the United Kingdom, court approval is required for a DPA, which means that even if the SFO recommends a DPA after extensive co-operation, the court may reject it.

& Gas Limited v. Director of the Serious Fraud Office[77] provides an illustration of the expense, difficulty and disruption associated with seeking to force the SFO to bring about a conclusion to an investigation. Corporates therefore need to evaluate the risks and costs inherent in making self-reports very carefully. Some key risks and practical considerations are set out below.

Interest and potential investigation in other jurisdictions 3.5.2.1

There is always a risk of contagion: it is the nature of complex bribery, fraud and corruption that it crosses borders and can implicate authorities in multiple jurisdictions. Self-reporting to a regulator in one jurisdiction may draw the attention of other regulators, domestically or abroad. Matters are frequently complicated because the benefits and risks of reporting are seldom consistent or certain across jurisdictions, and authorities in different countries seldom have the same procedures, techniques or demands in conducting their investigations and taking enforcement action.

Increasingly, regulators are sharing information and seeking to collaborate in enforcement actions. As long ago as 2010, the US Department of Justice (DOJ) and the SFO worked together in investigating BAE Systems plc,[78] and such co-operation has since become routine. International co-operation often goes beyond formal mutual legal assistance requests, to encompass informal intelligence sharing (sometimes in advance of formal investigation in any jurisdiction), coordination or division of responsibility or issues for enforcement, and even formal programmes by which to enhance understanding and assist with capacity or resourcing. At a symposium in September 2016, Sir David Green QC, then Director of the SFO, explained: 'All [SFO] cases have a significant international dimension. We have invested real effort in building strong co-operative relations with foreign agencies in key financial centres across the globe. This involves secondments, rolling discussions, exchange of information and coordinated activity.'[79]

While there are legal limits to the extent of information sharing and collaboration between authorities, firms need to be strategic in their conduct across all countries. It is important to take heed of cases such as *United States v. Allen*,[80] in which the US Court of Appeals for the Second Circuit held that the prohibition against the use (and derivative use) of a defendant's compelled testimony will apply even where the testimony had been compelled by a foreign authority, such as the FCA. The DOJ therefore needs to ensure that it avoids its own investigation becoming 'tainted' by compelled testimony when it is collaborating or exchanging

77 *Soma Oil & Gas Limited v. Director of the Serious Fraud Office* [2016] EWHC 2471 (Admin).

78 See the DOJ's expression of gratitude to the SFO for its assistance in its press release, March 2010, available at www.justice.gov/opa/pr/bae-systems-plc-pleads-guilty-and-ordered-pay-400-million-criminal-fine.

79 Sir David Green QC, former Director of the SFO, speech at the Cambridge Symposium on Economic Crime 2016 at Jesus College, Cambridge, 5 September 2016, available at www.sfo.gov.uk/2016/09/05/cambridge-symposium-2016/.

80 *United States v. Allen*, No. 16-898 (2d Cir. 2017).

information with other countries' authorities – a particular concern as regards the United Kingdom, where the provision of evidence or interviews is commonly compelled. This also means that there is a risk that, by providing to the DOJ reports or information derived from compelled testimony (even by inadvertence, as part of routine updates or reports on progress or developments in parallel investigations), a firm may risk negating any co-operation credit that they might have established in other ways.

3.5.2.2 Privilege issues and authorities' involvement in the internal investigation

Legal advice in relation to internal investigations

A key concern for all firms considering and investigating suspicions or allegations of wrongdoing is to establish clearly at the outset that its board, or any committee with oversight of internal investigations, is authorised to seek and receive legal advice in relation to the investigation to ensure that updates to these bodies and related documents will be protected by legal professional privilege. This authorisation is important because English law on the question of who is the 'client' for the purposes of legal professional privilege remains rooted in the House of Lords decision in *Three Rivers No. 5*, such that the 'client' was not the corporation itself but only those officers and employees of the corporation who were 'authorised' to communicate with the corporation's lawyers.[81] In its September 2018 judgment in the *ENRC* case, the Court of Appeal made a number of interesting comments on the latter rule. The court noted in particular that this rule was more appropriate for the 19th century than the 21st century, that its application may result in a disadvantage to modern multinational corporations (where the information required to obtain legal advice would often be in the hands of people not charged with obtaining it),[82] and that it would have been in favour of departing from *Three Rivers No. 5* if it had been open to it to do so. Significantly, however, those comments were *obiter* on the basis that only the Supreme Court can reverse or depart from the decision in *Three Rivers No. 5*.

Material generated during internal investigations

A significant concern in the context of internal investigations centres on the material generated during an internal investigation, including any investigation work and work-product that may have preceded the self-report. This material typically includes interview notes and summaries of key documents and issues.

The UK authorities are adamant that to self-report in any meaningful sense, firms must provide them with sufficiently detailed information about the wrongdoing. The SFO states: 'All supporting evidence including, but not limited to emails, banking evidence and witness accounts, must be provided to the SFO's

81 *Three Rivers District Council and Others v. The Governor and Company of the Bank of England* [2003] EWCA Civ 474 (*Three Rivers No. 5*).

82 Especially as compared with smaller corporations, which the Court noted was the typical size and structure of the corporations involved in the 19th century cases considered in *Three Rivers No. 5*.

Intelligence Unit as part of the self-reporting process.'[83] In practice, the SFO's Intelligence Unit will not always want every email that has been identified during an internal investigation. A key question for a company considering a self-report is thus whether or not it is prepared to disclose its full interview notes; the privileged status of which has been subject to heated debate in the United Kingdom in recent years.

By way of context, a good starting point is the April 2018 decision of the High Court in *R (AL) v. Serious Fraud Office*.[84] The case arose out of the SFO's investigation of Sarclad, during which the SFO had accepted 'oral proffers' of the first account interviews that had been conducted by an external law firm engaged by the company to conduct an internal investigation.[85] Having entered into a DPA with the corporate entity in 2016, the SFO turned its attention to a number of individuals, including the anonymised AL,[86] whose defence team repeatedly asked the SFO to obtain the complete notes of his first account interview with the law firm. The SFO asked Sarclad to disclose the interview notes but ultimately accepted the firm's refusal to do so on the grounds of privilege. Despite declining to exercise its judicial review jurisdiction (as it felt that disclosure disputes were best dealt with in the Crown Court), the High Court took the unusual step of stating that if it had chosen to exercise its judicial review jurisdiction, it would have found for AL. In *obiter* comments, Mr Justice Green, giving the judgment of the court, was critical of the SFO's acceptance of the law firm's claims that the current law of privilege was unclear pending the (then undecided) *ENRC* appeal. In Green J's view, the 'law as it stands today is settled. Privilege does not apply to interview notes.' In support of that statement, Green J cited the decision in *Three Rivers No. 6* and concluded that the SFO had 'erred' as it had 'simply accepted the assertion of privilege made by [the law firm] even though it is the SFO's own case that privilege does not apply and the SFO's position is supported by current case law', and that the SFO had therefore not fulfilled its duty to 'assess claims of privilege properly and not cursorily and superficially.'

The thrust of the *Sarclad* decision appeared to be in line with Mrs Justice Andrews' first instance decision in *ENRC*. However, as noted already, a few months later, in September 2018, the Court of Appeal overturned her decision and handed down a judgment that does not sit comfortably with *Sarclad*.[87] The Court of Appeal rejected Andrews J's decision that litigation privilege will only apply in criminal or regulatory proceedings at the point where a company had uncovered evidence of wrongdoing that meant that a criminal prosecution or enforcement again was likely to follow. The Court of Appeal reiterated the established principle that litigation privilege may be claimed over documents that had

83 www.sfo.gov.uk/publications/guidance-policy-and-protocols/corporate-self-reporting/.

84 *R (AL) v. Serious Fraud Office* [2018] EWHC 856 (Admin).

85 This was confirmed to be McGuireWoods.

86 Subsequently identified as Adrian Leek.

87 *Director of the Serious Fraud Office v. Eurasian Natural Resources Limited (Law Society intervening)* [2018] EWCA Civ 2006.

been created at a time when litigation was in 'reasonable contemplation' and for the purposes of that litigation. Such determinations are necessarily fact-specific. Notably, the Court of Appeal held that, on the *ENRC* facts, the interview notes generated during the course of its internal investigation were subject to litigation privilege on the basis that (1) they had been brought into existence after ENRC's external counsel (who were conducting an investigation) had advised that there was a real and serious risk of law enforcement and regulatory intervention, including criminal prosecution, and (2) the notes were, in the Court of Appeal's estimation, drafted to assist any future defence of such proceedings.

If a further illustration of the potential complexities and follow-on implications of DPAs were needed, it is provided by *Omers Administration Corporation and others v. Tesco PLC*.[88] In a judgment handed down in January 2019 in civil proceedings pursued by investors in respect of losses they claim resulted from the conduct forming the basis of the DPA agreed between the SFO and Tesco Stores Limited, Mr Justice Hildyard ordered disclosure of documents in the possession or control of Tesco PLC. These included some documents provided to it by the SFO that had been obtained from third parties through the use of the SFO's compulsory powers under section 2 of the Criminal Justice Act 1987 and transcripts of interviews with and witness statements of third parties. The conflict between Tesco PLC's obligations to keep these documents confidential pursuant to an undertaking provided to the SFO as part of the DPA negotiation process, and its disclosure obligations in the follow-on litigation pursued by investors under the Financial Services and Markets Act 2000, generated substantial ancillary litigation and a costly and involved process of seeking representations from third parties. The proceedings serve as a reminder that although a DPA may avoid the need for protracted criminal proceedings, it provides no guarantee of finality in respect of (and indeed may provide oxygen for) associated civil (or regulatory) proceedings.

The SFO has maintained for some time that firms wishing to co-operate with the SFO need to give serious consideration to waiving privilege, and that it is ready to challenge any overly broad claims to privilege. The Corporate Co-operation Guidance reinforces that approach. It notes that a claim to privilege must be properly established, that any claim should be supported by independent counsel and that the Court of Appeal in *ENRC* 'has not ruled out a court's consideration of the effect of an organisation's non-waiver over witness accounts as it determines whether a proposed DPA is in the interests of justice'.[89]

Following the Court of Appeal judgment in *ENRC*, it is open to any company that has conducted an initial investigation and received clear legal advice that the information unearthed may amount to a criminal offence or a regulatory failing[90]

88 *Omers Administration Corporation and others v. Tesco PLC* [2019] EWHC 109 (Ch).

89 SFO Operational Handbook, Corporate Co-operation Guidance, p. 1 at note 5, citing *The Director of the Serious Fraud Office v. ENRC* [2018] EWCA Civ 2006 at para. 117, available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

90 Indeed it is not clear on what other basis such a company would self-report.

to claim that any material generated in the course of that initial internal investigation will be subject to litigation privilege.

In practice, however, and especially following the publication of the Corporate Co-operation Guidance, companies are likely to come under pressure from the SFO to disclose interview transcripts as part of the self-reporting process. The Court of Appeal's judgment in *ENRC* made it clear that nothing it said about privilege should adversely impact the DPA regime and, furthermore, that maintaining claims to privilege may adversely affect prospects of obtaining a DPA.[91] The Court also noted: 'Had the court been asked to approve a DPA between ENRC and the SFO, the company's failure to make good on its promises to be full and frank would undoubtedly have counted against it.'[92]

In deciding whether to acquiesce in providing witness accounts, a company will need clear advice as to the risks involved in waiving litigation privilege, even on a limited basis, at such an early stage, particularly before it is clear whether a settled resolution is likely and especially where multiple authorities may be involved. The shield of litigation privilege is clearly of paramount importance to any company defending criminal or regulatory enforcement proceedings where, very commonly, civil litigants will be waiting in the wings and in jurisdictions where the concept of limited waiver may not exist.

See Chapter 35 on privilege

Involvement of authorities in internal investigation

Having ensured that the internal investigation is suitably established for the purposes of privilege, another critical concern for any corporate will be the likelihood of potential involvement in, or loss of control of the scope, timing and conduct of, its own investigation into the matters concerned. The former Director of the SFO, Sir David Green QC, made it clear that the SFO might specify particular areas or issues to be included in the firm's investigation, how the investigation ought to be conducted in relation to particular issues or persons, and to provide updates to the SFO, usually within agreed time frames.[93] Sir David Green QC explained the SFO's influence or imposition into internal investigations as being necessary to avoid 'churning up the crime scene' and compromising the SFO's own investigation. This, again, is reinforced in the Corporate Co-operation Guidance.

Similar sentiment (if not criticism) was expressed by Mark Steward, the FCA's Head of Enforcement, who referred to 'the crime scene being trampled over'. While he was Director of the SFO, in June 2016, Sir David Green QC also suggested that the SFO's influence or control over internal investigations might usefully be formalised so that it would be akin to the FCA's use of 'skilled persons

91 *Director of the Serious Fraud Office v. Eurasian Natural Resources Limited (Law Society intervening)* [2018] EWCA Civ 2006, at paras. 115 to 117.

92 Ibid.

93 Sir David Green QC, former SFO Director, speech at GIR Roundtable Discussion on Corporate Internal Investigations, 27 July 2015.

investigations' (also known as section 166 investigations) of regulated firms.[94] The latter involves the FCA requiring the firm to engage (and pay for) an independent 'skilled person' (typically a law firm or forensic accountants, depending on the subject matter), approved by the FCA, to investigate and report to the FCA on areas or issues of concern specified by the FCA.[95]

This approach and degree of involvement in internal investigations by UK authorities is far greater than is the case in the United States, where authorities allow (if not encourage) firms to conduct internal investigations without much intrusion, on the basis that they can provide direction where necessary and that the firms will share the output and provide updates at agreed points.

3.5.2.3 Impact on witness interviews

In addition to influencing the scope of an internal investigation, UK authorities may also influence a firm's ability to conduct witness interviews after self-reporting, whether by prohibiting the firm from conducting interviews with certain individuals, or by requiring the firm to delay such interviews until after the authority has interviewed the individuals concerned. In approving the various DPAs to date, Sir Brian Leveson highlighted the assistance provided by firms to the SFO in relation to witness interviews. In relation to the Rolls-Royce DPA, for example, Leveson P noted the high levels of co-operation from Rolls-Royce as regards its witnesses, pointing out that when the SFO commenced its own investigation, not only did it have access to Rolls-Royce's internal investigations and interview notes (Rolls-Royce having made a limited waiver of its claims for legal professional privilege over them), but Rolls-Royce also deferred certain interviews until after the SFO had completed interviews of them.

3.5.2.4 Scrutiny, including potential monitoring obligations

A DPA or settled resolution will always include a number of non-financial terms and conditions. While these will often be fact-dependent and tailored to the wrongdoing involved and the state of the firm's remediation at the point of agreement, the DPA Code includes a list of terms that may be agreed as part of a DPA, including requirements for putting in place a robust compliance or monitoring programme, or both, which may include the appointment of an independent monitor.[96]

While the imposition of a corporate monitor is not compulsory, the DPA Code provides lengthy guidance as to monitors' roles and appointment, and notes that the imposition of a monitor 'must always be fair, reasonable and proportionate'.[97]

---

94 Sir David Green QC, former SFO Director, speech at a Q&A session organised by The Fraud Lawyers Association and the European Fraud and Compliance Lawyers Association in London, 17 June 2016 (see http://globalinvestigationsreview.com/article/1036163/david-green-sfo-can-learn-from-fca-approach-to-internal-investigations).

95 Financial Services and Markets Act 2000, s.166.

96 DPA Code, para. 7.10(iii).

97 DPA Code, paras. 7.11 to 7.22.

Where a monitor is required, the costs to the firm can be significant. Not only will the firm have to pay the monitor's fees, but it will also have to pay the costs associated with the selection, appointment and reasonable 'monitoring' costs of the prosecutor during the monitoring period. There are indirect or non-financial costs, too. The monitor must be given complete access to all relevant aspects of the firm's business and the firm will need to allocate resources to ensure that the monitor is provided with the information and co-operation required and to establish the systems and controls necessary to effect the remediation agreed with the regulator.

These costs have attracted a degree of judicial and corporate scepticism and criticism in the United Kingdom and the United States. In the *Innospec* case,[98] for example – where a UK subsidiary agreed with the SFO to plead guilty to corruption charges as part of the first 'global settlement' relating to similar conduct prosecuted by US authorities against its parent entity, and the first joint US–UK monitor was appointed – District Judge Huvelle gave a colourful criticism of the role of monitors, saying: 'It's an outrage that people get US$50m to be a monitor . . . . It's a boondoggle for some of these people.'[99] Lord Justice Thomas (the judge in the English case) chose instead to characterise the imposition of a monitor as 'an expensive form of "probation order"', which he considered 'unnecessary for a company which will also be audited by auditors well aware of the past conduct and whose directors will be well aware of the penal consequences of any similar criminal conduct'.[100]

See Chapter 32 on monitorships

Such criticism notwithstanding, the appointment of a monitor (in one form or another) is likely to feature regularly in DPAs in the future, as had previously been the case in civil recovery orders[101] or criminal court orders,[102] which were the SFO's preferred means of imposing monitorships before the introduction of the DPA regime provided it with a statutory basis for doing so. Indeed, in early 2017, the then SFO General Counsel, Alun Milford, explained that 'an integral part of any DPA discussion is the question of corporate reform. As such, monitors aren't something the SFO has set its face against, but as we've seen from the judgments, there are different ways of achieving that sort of process'.[103]

98 See https://www.sfo.gov.uk/cases/innospec-ltd/.

99 Christopher M Matthews, 'Judge Blasts Compliance Monitors at Innospec Plea Hearing,' (18 March 2010), https://globalinvestigationsreview.com/article/jac/1019218/judge-blasts-compliance-monitors-at-innospec-plea-hearing.

100 *R v. Innospec Ltd* [2010] Lloyd's Rep FC 462, at para. 49.

101 For example, the civil recovery orders between the SFO and Balfour Beatty plc in October 2008; Macmillan Publishers Ltd in July 2011; and Oxford Publishing Ltd in July 2012.

102 For example, in relation to Mabey & Johnson in September 2009, as well as Innospec Ltd in March 2010. See https://star.worldbank.org/corruption-cases/sites/corruption-cases/files/documents/arw/Mabey_Johnson_UK_SFO_Press_Release_Sentencing_Sep_25_2009.pdf and https://www.sfo.gov.uk/cases/innospec-ltd/, respectively.

103 Alun Milford, then SFO General Counsel, speech at GIR Live London in April 2017, www.globalinvestigationsreview.com/article/1144199/gir-live-london-dpas-the-new-normal.

The five DPAs reached to date clearly demonstrate this flexibility in the SFO's approach to monitorships. While the SFO required Standard Bank to commission and submit to an independent review of its existing compliance programme by PwC, and to implement PwC's recommendations (less onerous than a monitorship),[104] it did not require an independent monitor in its DPA with Sarclad, opting instead for a form of 'self-monitoring' for the first time, with the company's Chief Compliance Officer being required to report to the SFO on its anti-bribery and corruption policies and their implementation within one year, and annually for the duration of the DPA.[105] The approach in the Rolls-Royce DPA was different again – some four years before the DPA was agreed, Rolls-Royce had appointed Lord Gold to conduct an independent review of (and report on and make and oversee the implementation of recommendations regarding) the company's anti-bribery and corruption compliance infrastructure. In approving the DPA, which required the continuation of Lord Gold's work and the production by him of a final report to the SFO after implementation, Leveson P described Lord Gold as a 'quasi monitor'.[106] The Tesco Stores DPA required the appointment of Deloitte as an independent monitor to conduct a review, provide a report and implement recommendations in relation to a number of specific areas of concern.[107] In the DPA agreed in July 2019 between the SFO and Serco Geografix Limited, the company is required to report 'evidence of fraud by itself or related companies or individuals' and to take steps to enhance and report annually on the effectiveness of its ethics and compliance programme. Some corresponding reporting and enhancement requirements were also imposed on its parent company.

The current Director of the SFO, Lisa Osofsky, is very familiar with monitorships, and it is likely that she will be in favour of increasing their use, even if implemented in the United Kingdom as quasi-monitorships.

3.6 Practical considerations, step by step

3.6.1 Reaching the decision

Sometimes the decision to self-report may be clear-cut or the only sensible option (particularly where a whistleblower has made serious allegations). More often, however, it will be necessary to conduct an internal investigation to test the information underlying the concerns and to ensure that any report made to authorities

104 PwC was given the role of producing a report on Standard Bank's anti-bribery and corruption systems, controls, policies and procedures, the recommendations in respect of which the bank was then obliged to implement (to PwC's satisfaction) and within a year of that report. *Serious Fraud Office v. Standard Bank plc*, available at www.judiciary.uk/wp-content/uploads/2015/11/sfo-v-standard-bank_Final_1.pdf.

105 *Serious Fraud Office v. XYZ Limited* (Case No. U20150856) [2016] 7 WLUK 220; [2016] Lloyd's Rep FC 509.

106 *Serious Fraud Office v. Rolls-Royce plc and Rolls-Royce Energy Systems Inc.* (Case No. U20170036) [2017] Lloyd's Rep FC 249, at para. 43.

107 FCA Final Notice, Tesco plc and Tesco Stores Ltd (28 March 2017), at para. 4.10, available at www.fca.org.uk/publication/final-notices/tesco-2017.pdf.

is as complete and accurate as possible. How long this takes will depend on a range of factors, including where and when the alleged conduct took place, how many individuals are alleged to have been involved, and the availability of relevant documents and individuals for interview. It is critical to ensure that the decision to self-report is taken by directors who are independent of the underlying events or issues, and that the decision is taken in conjunction with appropriate legal advisers and is suitably documented. One of the first steps in this process must be to immediately preserve all relevant documents, and to ensure that the investigation is carefully scoped and proceeds expeditiously.

There is no one 'correct' approach to investigating disclosures, allegations or whistleblowers' reports. What is necessary and appropriate when following up on a disclosure will vary significantly depending on factors including the jurisdictions, personnel and business areas implicated. Several key principles may, however, help corporates to respond decisively and consistently, and to protect their interests when they receive disclosures of alleged misconduct.

Clear communication 3.6.1.1

Clear communication underpins a successful response to a disclosure, particularly where a whistleblower is involved. Carefully delineated channels must be in place to enable staff receiving disclosures (whether through a dedicated hotline or other less formal channels) to escalate them quickly and to the right people. In particular, policies and procedures should name a designated member of the senior management of the corporate (probably in its legal or compliance function) who should have a direct reporting line to the board or audit committee. Provision should also be made for how to deal with disclosures naming members of the board or the designated senior manager responsible for handling whistleblowing reports.

Even, dispassionate investigation 3.6.1.2

Not every disclosure or whistleblowing report will justify the expenditure of time and resources on comprehensive internal investigations or involve reports to authorities. It is clearly important to guard against complacency or undue cynicism when evaluating issues, or reports by whistleblowers. Level-headedness and even-handedness pay dividends. Allegations should be viewed dispassionately and, where possible, empirically tested by reference to readily available documents, or by means of interviews with relevant individuals (who should be apprised of the importance of confidentiality).

Clear protocol and structure 3.6.1.3

Where initial enquiries show disclosures or allegations to be well founded, firms' responses should be guided by clear protocols. These should set out the circumstances in which external legal counsel should be instructed (which may well be advisable at an early stage to ensure the preservation of any applicable privilege, as discussed above). They may also deal with how and when other external specialist resources (such as forensic IT consultants or accountants) may be required and

instructed, and how such selection and instruction should occur (which should involve instruction by legal counsel, again to maintain privilege as far as possible).

Appropriate senior individuals within the organisation's human resources function should also be identified to coordinate its approach towards the whistleblower (if there is one) and to deal with any disciplinary action in relation to other employees that may be necessary. The FCA and PRA's whistleblowing rules require some regulated firms to have enhanced their existing whistleblowing procedures, including the appointment of a whistleblowers' champion since 7 March 2016.

3.6.1.4 Senior management involvement

Once notified of the fact of serious issues or allegations made in a whistleblowing report, it is paramount that the firm's senior management is kept apprised of the progress of enquiries. Once evidence emerges that establishes that complaints appear to be well founded, the window within which firms may receive maximum credit for self-reporting actual or suspected misconduct to the appropriate authorities is relatively short.

3.6.2 Once the decision has been made

Where corporates determine that it is necessary to make a report to authorities, the main challenges facing them are to demonstrate that any self-report (1) has been made in a timely fashion, (2) has been made genuinely voluntarily (i.e., not simply because public disclosure or a regulatory or criminal investigation is imminent), and (3) contains enough information to enable the authority to make a meaningful and informed assessment as to how to proceed.

A firm should aim to be the first to self-report to maximise credit. Generally, authorities will acknowledge that internal investigations into complex matters that may have occurred many years ago take time and give credit for initial notifications based on certain key facts having been established, with an indication that a fuller report will follow the completion of a more thorough investigation.

3.6.3 Documenting the decision

Regardless of whether the decision is to report or not, it is important for the firm's board to ensure that the issue or allegation is investigated, properly considered with appropriate advice and properly documented. The board must also ensure that appropriate remediation steps are taken, not only to mitigate the risks of criminal, regulatory and civil action, but also to demonstrate the firm's cultural responsiveness and change.

Firms must be careful in documenting the steps taken in reaching their decisions, so as to preserve privilege as far as possible and with regard to the likelihood of such documentation subsequently becoming subjected to external scrutiny or publicity, the latter being particularly likely where the firm is a public company.

Nature of approach to the authorities 3.6.4

Self-reports to authorities are not generally made in a set format, but instead usually take the form of a preliminary notification (typically verbal) soon after receiving notice of potential wrongdoing followed by a more detailed written or oral report after further investigation. The nature and scope of disclosures to authorities vary significantly between, and often within, jurisdictions and may depend on whether the issues cross borders. Specifically, whether it is possible to preserve any applicable privileges by providing reports orally rather than in writing will depend on the circumstances.

Timing of approach (DPAs) – what is a reasonable time? 3.6.5

The SFO requires self-reporting to be made within a reasonable time of an organisation becoming aware of the issue, and certainly before the SFO becomes aware of it by some other means, and before the firm is threatened with investigation or action by other bodies or authorities, including threatened leaks to the press.

Beyond the impact it may have on securing a DPA, the timing of a self-report will also have a bearing on the decision to prosecute and the level of any potential penalties. The Sentencing Council Definitive Guideline states that concealing an offence may result in the imposition of heavier penalties. The Guidance on Corporate Prosecutions expressly states that failing to report within a reasonable time will be a 'public interest' factor weighing in favour of prosecution, whereas a 'genuinely proactive approach involving self-reporting and remedial action' will be a factor tending against prosecution.[108]

The SFO's expectations as regards timing has become somewhat more realistic over time. The former SFO Director, Sir David Green QC, had stated in 2013 that '[c]ommon sense suggests that an initial report of suspected criminality should be made to the SFO as soon as it is discovered'.[109] Some three years later (in March 2016), the then SFO General Counsel, Alun Milford, said that it is reasonable for a firm to undertake an initial assessment before doing so,[110] a view that was echoed three months later by Matthew Wagstaff, SFO Joint Head of Bribery and Corruption, when he said that it is unrealistic to expect a firm to pick up the telephone to the SFO at the very moment it first becomes aware of potential wrongdoing.[111] In March 2018, Camilla de Silva, the SFO Joint Head of Bribery and Corruption, commented that the SFO 'will not be offering DPAs

108 Bribery Act 2010: Joint Prosecution Guidance of The Director of the Serious Fraud Office and The Director of Public Prosecutions (30 March 2011).

109 Sir David Green QC, former SFO Director, speech at the Pinsent Masons and Legal Week Regulatory Reform and Enforcement Conference, 24 October 2013, available at www.sfo.gov.uk/2013/10/24/pinsent-masons-legal-week-regulatory-reform-enforcement-conference-2/.

110 Alun Milford, then SFO General Counsel, speech at the European Compliance and Ethics Institute, Prague, on 29 March 2016, available at www.sfo.gov.uk/2016/03/29/speech-compliance-professionals/.

111 Matthew Wagstaff, SFO Joint Head of Bribery and Corruption, speech at the 11th Annual Information Management, Investigations Compliance eDiscovery Conference, London, on 18 May 2016, available at www.sfo.gov.uk/2016/05/18/role-remit-sfo/.

in cases of a late conversion to the joys of co-operating; DPAs are a reward for openness – the sooner you come in, self-report and the more you are open with us, the more you have to be rewarded for'.[112] In speeches to date, Lisa Osofsky has indicated that the SFO will be open to firms investigating allegations of misconduct before reporting.[113]

3.6.6 Managing other regulators

Whatever format is used to report matters to authorities, corporates and their advisers should assume that information provided to one enforcement authority will be passed to others, and that referrals may be made where authorities have parallel jurisdiction over some or all aspects of the corporate's activities. In cases where the SFO does not prosecute a self-reporting corporate, the SFO reserves the right to prosecute the firm for any unreported violations of the law, and may provide information on the reported violation to other bodies (such as foreign police forces or authorities) through the relevant gateway.

The above notwithstanding, corporates should not assume that disclosure to one authority necessarily means that other relevant authorities are aware of the matter – full assessments must be made as to whether it is necessary or appropriate to make separate notifications to other specific authorities (whether in the same jurisdiction or elsewhere) who might expect to be told of the alleged misconduct or of the fact of other investigations by or at the behest of enforcement authorities.

112 Camilla de Silva, SFO Joint Head of Bribery and Corruption, speech at ABC Minds Financial Services conference, 15 March 2018, available at www.sfo.gov.uk/2018/03/16/camilla-de-silva-at-abc-minds-financial-services/.

113 Lisa Osofsky, SFO Director, speech at the American Bar Association's London White Collar Crime conference alongside Sandra Moser (acting chief of the DOJ's Fraud Section), 8 October 2018.

4

Self-Reporting to the Authorities and Other Disclosure Obligations: The US Perspective

Amanda Raad, Sean Seelinger, Jaime Orloff Feeney and Zaneta Wykowska[1]

Introduction 4.1

There is typically no formal obligation in the United States to disclose potential wrongdoing to enforcement authorities; however, there can often be strategic advantages to doing so. Subjects of investigations may, in certain cases, avoid some of the most adverse consequences by self-reporting, including reduced penalties and more favourable settlement terms. Additionally, companies in certain regulated sectors may avoid debarment even where clear violations occurred. US regulators are incentivising companies to self-report by offering potential and meaningful co-operation credit for doing so. The Corporate Enforcement Policy of the US Department of Justice (DOJ), first announced in November 2017, updated and formalised the DOJ's criteria for evaluating and rewarding self-disclosure and co-operation in cases relating to the Foreign Corrupt Practices Act (FCPA). Revisions in March and November 2019 broadened its application beyond the FCPA and clarified the DOJ's expectations for securing credit.

Despite public perception to the contrary, the Trump administration appears committed to enforcing the FCPA, including a continued focus on self-reporting and multi-jurisdictional co-operation. In 2017, the DOJ brought 29 FCPA actions and the SEC brought 10, with a total of US$958 million in monetary sanctions. In 2018, the DOJ brought 20 enforcement actions and the SEC brought 17, netting a combined US$2.2 billion in fines. The DOJ is on track to match or surpass that total this year, with US$1.56 billion in monetary fines up to October 2019. The DOJ's March 2019 settlement with Mobile Telesystems and

1 Amanda Raad is a partner, Sean Seelinger is counsel, and Jaime Orloff Feeney and Zaneta Wykowska are associates, at Ropes & Gray LLP.

its Uzbek subsidiary[2] was one of the largest in an FCPA case – US$850 million to resolve charges arising out of a scheme to pay bribes in Uzbekistan.

Moreover, US regulators have historically been receptive to parties reporting facts while preserving privilege during the co-operation and reporting process, and are specifically prohibited from making co-operation credit conditional on privilege waiver.

4.2 Mandatory self-reporting to authorities

Before considering a voluntary disclosure, it is important for at least two reasons to determine whether the company has any potential mandatory reporting obligation. First, mandatory reporting obligations often prescribe the recipient, form, timing and content of the disclosure. Second, the evaluation will be materially different if a mandatory report is required, even if that report is in another jurisdiction, given the clear commitment to sharing information between international regulators. In other words, if a company is required to self-report in at least one jurisdiction, it should consider voluntarily disclosing in others given the likelihood that the government agencies will share information.

See Chapter 24 on negotiating global settlements

In May 2018, the DOJ announced a new formal policy to avoid 'piling on' penalties that are duplicative for the same misconduct. Under the policy, various US enforcement agencies must coordinate with each other and with foreign government agencies when reaching settlements with corporations. However, the DOJ has warned that companies looking to benefit from the new policy should self-disclose wrongdoing to the DOJ. When announcing the policy, former Deputy Attorney General Rod Rosenstein specifically remarked that the DOJ 'will not look kindly on companies that come to [the DOJ] after making inadequate disclosures to secure lenient penalties with other agencies or foreign governments. In those instances, the Department will act without hesitation to fully vindicate the interests of the United States'.[3]

4.2.1 Statutory and regulatory mandatory disclosure obligations

In the United States, most disclosure obligations originate in statute or regulations. Key examples include:

- the Sarbanes-Oxley Act of 2002, which requires the disclosure of all information that has a material financial effect on a public company in periodic financial reports;

2 See 'Mobile Telesystems Pjsc and Its Uzbek Subsidiary Enter into Resolutions of $850 Million with the Department of Justice for Paying Bribes in Uzbekistan', available at https://www.justice.gov/opa/pr/mobile-telesystems-pjsc-and-its-uzbek-subsidiary-enter-resolutions-850-million-department.

3 Rod J Rosenstein, Deputy Att'y Gen., Dep't of Justice, Remarks to the New York City Bar White Collar Crime Institute (9 May 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

- the US Bank Secrecy Act of 1970, which requires financial institutions to disclose certain suspicious transactions or currency transactions in excess of US$10,000;
- the US Anti-Money Laundering Regulations, which require financial institutions to report actual or suspected money laundering under certain circumstances;[4]
- state data breach regulations – 47 of 50 US states have laws requiring companies conducting business in the state to disclose data breaches involving personal information; and
- the Anti-Kickback Enforcement Act of 1986, which requires government contractors to make a 'timely notification' of violations of federal criminal law or overpayments in connection with the award or performance of most federal government contracts or subcontracts, including those performed outside the United States.

Disclosure obligations under existing agreements with the government 4.2.2

In addition to statutory or regulatory-based mandatory disclosure requirements, companies must also evaluate whether they have any mandatory disclosure obligations under pre-existing agreements with the government. For example, if a company is subject to a deferred prosecution agreement (DPA) (or a corporate integrity agreement (CIA) in the healthcare sector), the agreement often contains self-reporting mandates for any subsequent violations. In many cases, these agreements may require the appointment of independent monitors. While DPAs, CIAs and similar agreements have been used frequently in the United States, other countries, including the United Kingdom, are also now increasingly using similar agreements to drive self-reporting and co-operation.

See Chapter 32 on monitorships

Other sources of mandatory disclosure obligations 4.2.3

Individuals and companies may also have mandatory disclosure obligations as a result of private contractual agreements as well as membership in professional bodies. Such disclosures between private parties may lead to a disclosure to a regulator by the receiving entity. For example, a subcontractor may be obliged by contract to report issues to the contracting party. That contracting party may subsequently determine that it is subject to its own reporting obligation or may choose to self-report to reduce any potential liability.

Voluntary self-reporting to authorities 4.3

Self-reporting and co-operation are important factors for both the DOJ and the US Securities and Exchange Commission (SEC) in deciding how to proceed with and resolve investigations and enforcement actions in cases involving corporations. Companies must carry out a fact-intensive and holistic inquiry in deciding whether to voluntarily self-report to US authorities. There is no one-size-fits-all

4 See, e.g., 31 U.S.C. 5318(g).

approach to this analysis, but those contemplating voluntarily disclosing misconduct to US authorities should keep certain considerations in mind.

Key Considerations in Resolving Enforcement Actions	
US Department of Justice	*US Securities and Exchange Commission*
• Self-disclosure and willingness to co-operate in the investigation • Disclosure of individuals substantially involved in or responsible for misconduct • Pervasiveness of wrongdoing within the corporation • Existence and effectiveness of a compliance programme • Meaningful remedial actions	• Self-reporting and investigation of misconduct • Effective compliance procedures and appropriate tone at the top • Whether the case involves a potentially widespread industry practice • Whether the conduct is ongoing

4.3.1 Advantages of voluntarily self-reporting

The primary benefit to self-reporting is to secure potentially reduced penalties through co-operation credit and, moreover, to maintain control over the flow of information to regulators. In recent years, US regulators have become increasingly vocal about the benefits of self-disclosure and co-operation, with the DOJ even formalising those benefits, first, in its FCPA Pilot Program (Pilot Program),[5] and subsequently the Corporate Enforcement Policy. Yet, co-operation, which inevitably goes hand in hand with a voluntary disclosure, imposes significant demands on corporations and is not without meaningful risk.

4.3.1.1 DOJ co-operation credit

To encourage self-reporting and co-operation, the DOJ has issued and subsequently revised guidance on the subject for many years. In June 1999, the DOJ issued the Principles of Federal Prosecution of Business Organizations, now known as the 'Holder Memorandum', to articulate and standardise the factors to be considered by federal prosecutors in making charging decisions against corporations.[6] The Holder Memorandum instructed DOJ prosecutors to consider as a factor in bringing charges whether a corporation has timely and voluntarily disclosed wrongdoing and whether it has been willing 'to cooperate in the investigation of its agents'.[7] In 2008, the then-Deputy Attorney General, Mark R Filip, added

5 For more details, see 'The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance', available at https://www.justice.gov/opa/file/838386/download (FCPA Enforcement Plan and Guidance).

6 Memorandum from Eric Holder, Deputy Att'y Gen., Dep't of Justice, on Bringing Criminal Charges Against Corps. to Dep't Component Heads and U.S. Attorneys (16 June 1999), available at https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2010/04/11/charging-corps.PDF.

7 Id. at 3 (listing eight factors prosecutors should consider in deciding whether to bring charges against corporations that include '[t]he corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents . . . .').

language to the US Attorneys' Manual, now titled the Justice Manual,[8] instructing prosecutors to consider 'the corporation's willingness to provide relevant information and evidence and identify relevant actors within and outside the corporation, including senior executives' when assessing a corporation's co-operation.[9] Mr Filip also outlined in his memorandum nine factors on which prosecutors base their corporate charging and resolution decisions, the so-called 'Filip Factors', incorporating some language from the Holder Memorandum (Filip Factor Four, a corporation's 'willingness to cooperate in the investigation of [its] agents'), and adding of Filip Factor Eight: 'the adequacy of prosecution of individuals responsible for the corporation's malfeasance'.[10]

The Yates Memorandum

Building on the Holder Memorandum, former Deputy Attorney General Sally Quillian Yates issued the Memorandum of Individual Accountability for Corporate Wrongdoing, now known as the 'Yates Memorandum', in September 2015.[11] The Yates Memorandum is still operative and outlines the 'six key steps' prosecutors should take in all investigations of corporate wrongdoing.[12] The most significant policy shift in the Yates Memorandum concerned the relationship between a company's co-operation with respect to individual wrongdoers and the company's eligibility for co-operation credit. Under the Yates Memorandum, the identification of responsible individuals became a 'threshold requirement' for receiving any co-operation credit consideration.[13] Ms Yates also emphasised that a failure to conduct a robust internal investigation is not an excuse, stating that '[c]ompanies may not pick and choose what facts to disclose'.[14] However, the revised Justice Manual clarifies that '[t]here may be circumstances where, despite its best efforts to conduct a thorough investigation, a company genuinely cannot get access to certain evidence or is actually prohibited from disclosing it to the government'.[15] Nevertheless, the Justice Manual is clear that in such cases 'the company seeking cooperation will bear the burden of explaining the restrictions it is facing to the prosecutor'.[16] Consequently, thorough and properly scoped internal investigations are of critical importance.

See Chapter 10 on co-operating with authorities

8 US Dep't of Justice, Justice Manual §§ 9-28.000.

9 Id. §§ 9-28.700 – Value of Cooperation.

10 Memorandum from Mark Filip, Deputy Att'y Gen. Dept' of Justice, Principles of Federal Prosecution of Business Organizations (28 August 2008), available at https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf, at 4.

11 Memorandum from Sally Quillian Yates, Deputy Att'y Gen., Dep't of Justice, Individual Accountability for Corporate Wrongdoing (9 September 2015), available at http://www.justice.gov/dag/file/769036/download, at 3. (Yates Memorandum).

12 The DOJ revised the section of the Justice Manual titled 'Principles of Federal Prosecution of Business Organizations' in November 2015 to reflect these steps.

13 Justice Manual § 9-28.700 (2015).

14 Yates Memorandum at 3.

15 Justice Manual § 9-28.700.

16 Id.

On 29 November 2018, former Deputy Attorney General Rod Rosenstein delivered a speech to FCPA practitioners announcing a shift in the DOJ's policy on co-operation credit and the scope of disclosure with respect to culpable individuals.[17] According to Rosenstein, the Yates Memorandum's policy directing prosecutors to make co-operation credit dependent on the corporation's disclosure of 'every person involved in [the] alleged misconduct in any way, regardless of their role' 'impeded resolutions and wasted resources'. Investigations were delayed solely to collect information on low-level employees unlikely to be prosecuted. By contrast, under the new policy, a corporation is entitled to co-operation credit in criminal proceedings as long as it discloses 'all relevant facts known to it *at the time of the disclosure*, including as to any individuals *substantially* involved in or responsible for the misconduct at issue'.[18] The DOJ will also use this standard to determine which corporations are entitled to full co-operation credit in the context of civil enforcement. In addition, corporations facing civil enforcement are now eligible for partial co-operation credit if, at the very least, they 'identify all wrongdoing by senior officials' and 'meaningfully assist the government's investigation'.[19] Finally, recognising that monetary recovery is the main objective of civil enforcement, the DOJ will once again let prosecutors 'consider an individual's ability to pay in deciding whether to pursue a civil judgment' – with the hope that prosecutors will avoid targets 'unlikely to yield any benefit'. Altogether, the new policy seeks to conserve 'limited investigative resources' while advancing traditional agency goals like deterrence and recovery and continuing to prioritise individual prosecution.

The Pilot Program and Corporate Enforcement Policy

In April 2016, the DOJ announced that it was launching a one-year Pilot Program to enhance its efforts to detect and prosecute individuals and companies for violations of the FCPA.[20] The Pilot Program, which incentivised voluntary self-disclosure of misconduct, was extended for an additional year on 10 March 2017. On 29 November 2017, former Deputy Attorney General Rod Rosenstein publicly applauded the Pilot Program as a 'step forward in fighting corporate crime' and announced that the DOJ would be incorporating a revised Corporate Enforcement Policy into the Justice Manual.[21] On 1 March 2018, the DOJ announced that it would apply the Corporate Enforcement Policy as non-binding

17 Rod J Rosenstein, Deputy Att'y Gen., Dep't of Justice, Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

18 See FCPA Corporate Enforcement Policy, Dep't of Justice, Justice Manual, §9-47.120, available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120 (Corporate Enforcement Policy) (emphasis added).

19 Supra note 17.

20 See FCPA Enforcement Plan and Guidance.

21 See Corporate Enforcement Policy.

guidance in criminal cases outside the FCPA context.[22] In light of this recent development, the Corporate Enforcement Policy provides valuable guidance to corporations as they investigate misconduct and contemplate voluntary disclosure.

The Corporate Enforcement Policy outlines factors that a company must meet to earn credit for voluntary self-disclosure. The disclosure (1) must occur prior to an imminent threat of disclosure or government investigation, (2) must be disclosed within a reasonably prompt time after the company becomes aware of the offence, and (3) must include all relevant facts known to the company at the time of disclosure, including all relevant facts about the individuals substantially involved in or responsible for the misconduct.[23] The November 2019 changes to the Corporate Enforcement Policy acknowledge the DOJ's recognition, in a footnote, that 'a company may not be in a position to know all relevant facts at the time of a voluntary self-disclosure.' The Corporate Enforcement Policy also now requires the company to alert the DOJ of evidence of the misconduct when it becomes aware of it, whereas, previously, where the company was or should have been aware of opportunities for the DOJ to obtain evidence not in the company's possession, it had to identify those opportunities to the DOJ in order to receive full co-operation credit.

The Corporate Enforcement Policy also contains specific guidance on the steps a company must take to earn full co-operation credit and to provide timely and appropriate remediation, consistent with the Yates Memorandum and the Justice Manual's Sentencing Guidelines. The exact level of co-operation credit available to a corporation will vary based on the investigation. It is possible for a corporation to earn full credit under the US Sentencing Guidelines but not earn additional credit under the Corporate Enforcement Policy.[24] Moreover, the DOJ has shown itself willing to assign different levels of co-operation credit for different investigations into the same company. For example, in June 2019, the DOJ entered an NPA with Walmart, resolving investigations into Walmart's alleged corrupt activity in four countries: Brazil, China, India and Mexico. Although the NPA covered conduct in all four countries, and the company received full credit for its co-operation with the DOJ in the first three investigations, with respect to the Mexico investigation, Walmart received only partial credit due to its failure to timely provide certain documents and 'deconflict' in response to a witness interview request.

See Chapter 10 on co-operating with authorities

Compared with the Pilot Program, the Corporate Enforcement Policy enhances the benefits available to a company that satisfies all the requirements for voluntary self-disclosure, co-operation and remediation. Under both programmes, companies that fully co-operate with DOJ investigations and implement appropriate

22 See Jody Godoy, 'DOJ Expands Leniency Beyond FCPA, Lets Barclays Off', *Law360*, 1 March 2018, https://www.law360.com/articles/1017798/doj-expands-leniency-beyond-fcpa-lets-barclays-off.

23 Corporate Enforcement Policy.

24 The DOJ evaluated corporate co-operation in this manner when reaching its DPA with Mobile TeleSystems in February 2019. See https://www.justice.gov/opa/press-release/file/1141631/download.

remediation in FCPA matters, but that do not voluntarily self-disclose, will be eligible for limited credit, at most a 25 per cent reduction off the bottom of the Sentencing Guidelines fine range. However, when a company has voluntarily self-disclosed, fully co-operated with the DOJ, and has timely and appropriately remediated, the Corporate Enforcement Policy creates a rebuttable presumption, which may be overcome by 'aggravated circumstances' related to the nature and seriousness of the offence, that the DOJ will grant a declination.[25] In contrast, the Pilot Program provided that the DOJ would 'consider' a declination for companies that met these requirements.[26] Under the Corporate Enforcement Policy, if the presumption is overcome and a criminal resolution is warranted, the DOJ will recommend a 50 per cent reduction off the low end of the Sentencing Guidelines fine range and generally will not require the appointment of a monitor if the company has, at the time of resolution, implemented an effective compliance programme.[27]

The DOJ issued seven public declinations under the Pilot Program and continues to decline prosecution under the Corporate Enforcement Policy.[28] Six declinations have been issued under the Corporate Enforcement Policy at the time of writing, with the most recent coming in February 2019, when the DOJ declined to prosecute Cognizant Technologies due to its voluntary self-disclosure, extensive co-operation and remediation, and disgorgement of US$19.37 million;[29] and in September 2019 when it issued a declination – in part for its prompt, voluntary disclosure of the misconduct – to Quad/Graphics,[30] which a week later agreed to disgorge approximately US$6.9 million of its ill-gotten gains to the SEC.[31]

All declination letters so far issued under the Corporate Enforcement Policy and Pilot Program have been publicly released by the DOJ. By publishing its rationale for issuing declinations, the DOJ has sought to provide 'increased transparency as to [the] evaluation process'.[32] However, in a June 2019 speech to

25 Corporate Enforcement Policy at § 1. 'Aggravating circumstances that may warrant a criminal resolution include, but are not limited to, involvement by executive management of the company in the misconduct; a significant profit to the company from the misconduct; pervasiveness of the misconduct within the company; and criminal recidivism.'

26 FCPA Enforcement Plan and Guidance, at 8-9.

27 Corporate Enforcement Policy at § 1. The Enforcement Policy provides specific guidance on the criteria for evaluating a corporate compliance programme, while also noting that the criteria may vary based on the size and resources of an organisation. Factors listed in the policy include culture of compliance, compliance resources, the quality and experience of compliance resources, independence and authority of the compliance function, effective risk assessments and risk-based approach, compensation and promotion of compliance employees, compliance-related auditing, and compliance reporting structure.

28 See https://www.justice.gov/criminal-fraud/pilot-program/declinations.

29 See https://www.justice.gov/criminal-fraud/file/1132666/download.

30 See https://www.justice.gov/criminal-fraud/file/1205341/download.

31 See https://www.sec.gov/news/press-release/2019-193.

32 Matt Miner, Deputy Assistant Att'y Gen., Dep't of Justice, Remarks at The American Bar Association, Criminal Justice Section Third Global White Collar Crime Institute Conference (27 June 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matt-miner-delivers-remarks-american-bar-association.

the American Bar Association, Deputy Assistant Attorney General Matt Miner announced that the DOJ would be open to keeping declinations private where public release is 'neither necessary nor warranted'. Miner gave the example of a corporation that discovers inconsequential bribes in the context of an M&A transaction and self-discloses immediately – in such a case, the agency would be 'open to discussion' regarding public release. Nonetheless, Miner maintained that this decision will always remain in the agency's discretion.

The following table compares several recent FCPA corporate resolutions under the Corporate Enforcement Policy, and the comparative credit for self-disclosure, co-operation and remediation.

Recent Resolutions under DOJ's Corporate Enforcement Policy	
Quad/Graphics Inc (Quad/Graphics)	
Background	Quad/Graphics is a US-based digital and print marketing provider. Between 2011 and 2016, employees of Quad/Graphics' Peruvian subsidiary paid or promised to pay over US$1 million to third-party intermediaries, in part, to pay bribes to Peruvian officials to secure printing contracts and minimise penalty and tax payments. Additionally, between 2010 and 2015, employees of Quad/Graphics' Chinese subsidiary paid bribes to employees of state-owned companies to secure printing business in China.
Self-Report	Quad/Graphics voluntarily and promptly self-disclosed to the DOJ.
Co-operation and Remediation	Quad/Graphics conducted an internal investigation, proactively co-operated with the DOJ, took steps to enhance its compliance programme and terminated relationships with employees and third parties involved in the misconduct.
Result	In September 2019, the DOJ issued a declination letter and the SEC issued a cease and desist order requiring Quad/Graphics to disgorge US$6.9 million in profits, plus interest and a US$2 million civil penalty.
TechnipFMC plc (TFMC)	
Background	TFMC, a global oil and gas technology and services company, was formed through a merger between Technip SA (Technip) and FMC Technologies, Inc (FMC Technologies). TFMC admitted that its predecessor companies engaged in two separate bribery schemes. Between 2003 and 2014, executives of Technip paid bribes to Brazilian officials through an intermediary, under the guise of legitimate consulting payments. Between 2008 and 2013, FMC Technologies paid bribes to government officials in Iraq to obtain contracts to provide metering technologies for oil and gas production.
Self-Report	TFMC did not self-report.
Co-operation and Remediation	TFMC received credit for substantial co-operation with the DOJ's investigation and for taking extensive remedial measures.
Result	In June 2019, TFMC entered into a DPA with the DOJ and agreed to pay a total criminal penalty of US$296 million to US and Brazilian authorities. The criminal fine included a 25 per cent reduction off the applicable US Sentencing Guidelines fine for co-operation and remediation.

(continues overleaf)

Recent Resolutions under DOJ's Corporate Enforcement Policy (cont.)	
Walmart Inc (Walmart)	
Background	Between 2000 and 2011, Walmart failed to implement sufficient anti-corruption related internal accounting controls. The failure to implement sufficient controls allowed Walmart subsidiaries in Mexico, Brazil, China and India to hire third-party intermediaries who made improper payments to government officials to obtain store permits and licences.
Self-Report	Walmart did not self-disclose the misconduct in Mexico and self-reported misconduct in India, Brazil and China only after the DOJ had already begun investigating the Mexico conduct.
Co-operation and Remediation	Walmart fully co-operated with the investigations in Brazil, China and India. Walmart co-operated with the investigation in Mexico, but did not timely provide documents and information to the DOJ and did not deconflict with the government's request to interview one witness before Walmart interviewed that witness.
Result	In June 2019, Walmart entered into a DPA with the DOJ in connection with a criminal information charging it with violations of the books and records provisions of the FCPA. Walmart entered into a related resolution with the SEC. Walmart agreed to pay US$137 million to resolve the DOJ's investigation, and to disgorge US$144 million in profits to the SEC. Walmart also agreed to retain an independent corporate compliance monitor for two years. Walmart received a 20 per cent reduction off the applicable US Sentencing Guidelines fine for conduct in Mexico, and a 25 per cent reduction for conduct in Brazil, China and India.
Cognizant Technology Solutions Corp (Cognizant)	
Background	Cognizant authorised its agents to pay an approximately US$2 million bribe to one or more government officials in India in exchange for securing and obtaining a statutorily required planning permit.
Self-Report	Cognizant voluntarily self-disclosed to the DOJ within two weeks of the board learning of the misconduct.
Co-operation and Remediation	Cognizant conducted a thorough investigation, fully and proactively co-operated with the DOJ, and took steps to remediate, including termination of employees and contractors involved in the misconduct. The DOJ also noted that the company had an effective pre-existing compliance programme and had taken additional steps to enhance its compliance programme and internal accounting controls.
Result	In February 2019, the DOJ issued a declination letter, while the SEC issued a cease and desist order requiring Cognizant to pay disgorgement of US$16.4 million, prejudgment interest of US$2.8 million and a US$6 million civil fine.

The Pilot Program and its codification as the Corporate Enforcement Policy has demonstrated the DOJ's commitment rewarding voluntary self-disclosure in FCPA enforcement, and by many accounts has been viewed as very successful.

Benczkowski Memorandum

As part of its ongoing effort to update and clarify its corporate enforcement policies, in October 2018, the DOJ issued new guidance on imposing corporate compliance monitors now known as the 'Benczkowski Memorandum'.[33] The new policy supplements the 2008 'Morford Memorandum', which outlined the principles on selection, scope and duration of monitorships, and supersedes the guidance contained in the 2009 'Breuer Memorandum' on imposing corporate monitors. Assistant Attorney General Brian Benczkowski explained that the goal of the new guidance was to 'further refine the factors that go into the determination of whether a monitor is needed, as well as clarify and refine the monitor selection process'.

Under the Benczkowski Memorandum, the potential benefits of employing a corporate monitor should be weighed against the cost of a monitor and its impact on the operations of the corporation. In making a determination to impose a corporate monitor, the DOJ will consider a number of factors, including the type of misconduct, the pervasiveness of the conduct and whether it involved senior management, the investments and improvements a company has made to its corporate compliance programme and internal controls, and whether those improvements have been tested to demonstrate that they would prevent or detect similar misconduct in the future. Other factors include whether remedial actions were taken against individuals involved, and the industry and geography in which the company operates and the nature of the company's clientele. The Benczkowski Memorandum provides: 'Where a corporation's compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will not be necessary.'[34]

The guidelines are clearly intended to complement the goals articulated in the Corporate Enforcement Policy, giving companies greater incentives to self-disclose and co-operate with DOJ investigations of corporate wrongdoing. A key feature of the Benczkowski Memorandum is that companies can receive meaningful credit, namely avoiding a compliance monitor, by engaging in extensive remediation of their compliance programmes.

See Chapter 32 on monitorships

33 Memorandum from Brian A Benczkowski, Assistant Att'y Gen., Dep't of Justice, (11 October 2018), Selection of Monitors in Criminal Division Matters, available at https://www.justice.gov/opa/speech/file/1100531/download (Benczkowski Memorandum); 'Assistant Attorney General Brian A. Benczkowski Delivers Remarks at NYU School of Law Program on Corporate Compliance and Enforcement Conference on Achieving Effective Compliance', available at https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-nyu-school-law-program.

34 Benczkowski Memorandum at 2.

4.3.1.2 SEC co-operation credit

Although it can be difficult to precisely quantify the benefit of co-operation with the SEC, the Commission will consider general principles of sentencing, especially general deterrence. In both public statements and in practice, the Commission has made clear that companies can receive significant leniency for full co-operation. During a speech on 9 May 2018, SEC Enforcement Division Co-Director Steven Peikin emphasised the importance of co-operation, noting that the SEC would continue to provide 'incentives to those who come forward and provide valuable information' to the SEC.[35] Co-operation may influence the Commission's decision whether to impose a civil monetary penalty.[36]

While the SEC has not entered into any non-prosecution agreements (NPAs) since 2016 and has only entered into three NPAs since their inception in 2010,[37] the SEC nevertheless signalled its continued commitment to using NPAs to reward co-operation through its proposed whistleblower rule amendments in 2018. Specifically, the proposed rule amendments would allow the SEC to make award payments to whistleblowers based on money collected as a result of DPAs and NPAs, to 'ensure that whistleblowers are not disadvantaged because of the particular form of an action' that the SEC or another regulator takes.[38] The SEC will, however, set a high bar before entering into an NPA in an FCPA enforcement action. With respect to NPAs entered into with Akamai Technologies, Inc and Nortek, Inc in 2016, Kara Brockmeyer, former Chief of the SEC Enforcement Division's FCPA Unit, stated: 'Akamai and Nortek each promptly tightened their internal controls after discovering the bribes and took swift remedial measures to eliminate the problems. They handled it the right way and got expeditious resolutions as a result.'[39]

4.4 Risks in voluntarily self-reporting

While self-disclosure can reap significant monetary benefits, a company must balance the potential risks against any potential benefit. Self-reporting can give rise to lengthy co-operation obligations and increased government scrutiny. As discussed

35 See 'Keynote Address at the New York City Bar Association's 7th Annual White Collar Crime Institute', available at https://www.sec.gov/news/speech/speech-peikin-050918.

36 In its November 2018 resolution with Vantage Drilling International, the SEC cited co-operation and financial condition as its basis for not imposing a fine. See https://www.sec.gov/litigation/admin/2018/34-84617.pdf.

37 The SEC announced its first NPA in an FCPA case in 2013, when it entered into an NPA with Ralph Lauren Corporation relating to bribes paid to government officials in Argentina. See 'SEC Announces Non-Prosecution Agreement With Ralph Lauren Corporation Involving FCPA Misconduct', available at https://www.sec.gov/news/press-release/2013-2013-65htm. The SEC announced its second and third NPAs on 7 June 2016. See 'SEC Announces Two Non-Prosecution Agreements in FCPA Cases', available at https://www.sec.gov/news/pressrelease/2016-109.html.

38 See 'SEC Proposes Whistleblower Rule Amendments', available at https://www.sec.gov/news/press-release/2018-120.

39 See 'SEC Announces Two Non-Prosecution Agreements in FCPA Cases', available at https://www.sec.gov/news/pressrelease/2016-109.html.

above, the multi-jurisdictional nature of many 'white-collar' matters means that self-reporting may lead to enquiries from global regulators, differing resolutions and ongoing obligations.

Furthermore, the DOJ is likely to impose a stringent bar when evaluating the sufficiency of compliance programmes to determine whether the requirements of the Corporate Enforcement Policy are met or to otherwise reduce liability. On 30 April 2019, the DOJ published revised guidance on Evaluation of Corporate Compliance Programs[40] (the Guidance). The Guidance is framed around three fundamental questions: (1) whether the corporation's compliance programme is well designed, (2) whether it is being implemented effectively and (3) whether it works in practice.

Although the content of the Guidance is largely familiar to practitioners, it does give a clearer picture of the DOJ's current approach to corporate compliance. The Guidance underscores the DOJ's focus on the operation, rather than the appearance, of corporate compliance programmes. The Guidance suggests that companies should expect to be asked detailed and challenging questions regarding the scope and effectiveness of their compliance programmes. If a company's compliance programme fails to withstand such scrutiny, it risks losing credit for the programme, paying higher penalties or even facing separate violations for inadequate internal controls. Taking these existing increasingly stringent co-operation standards into consideration, companies considering self-disclosure should carefully assess whether they can meet regulator expectations. If companies fall short, regulators may refuse co-operation credit and use the information obtained through the self-disclosure against the company.

Risks in choosing not to self-report 4.5

US regulators have warned that the potential downside of not self-reporting any violation could be significant where the matter is otherwise brought to their attention. In a 5 July 2018 press release announcing an NPA with a Hong Kong-based subsidiary of Credit Suisse Group to resolve an investigation into 'princeling' hiring by the bank, the DOJ noted certain steps the firm *did not take* that limited the amount of co-operation credit it received. Specifically, the bank did not receive voluntary disclosure credit and did not receive full co-operation credit because its 'cooperation was reactive and not proactive'.[41]

Consequently, companies should carefully consider the likelihood that the conduct will be discovered by other means. It is important to consider whether other industry players could affect the company's position. Industry-wide trends may expose a company's misconduct. If regulators undertake an industry-wide investigation into particular practices, which we have observed in recent years with pharmaceutical companies, medical device manufacturers and automobile

40 https://www.justice.gov/criminal-fraud/page/file/937501/download.

41 See 'Credit Suisse's Investment Bank in Hong Kong Agrees to Pay $47 Million Criminal Penalty for Corrupt Hiring Scheme that Violated the FCPA', available at https://www.justice.gov/opa/pr/credit-suisse-s-investment-bank-hong-kong-agrees-pay-47-million-criminal-penalty-corrupt.

companies, a company might be exposed by a competitor's self-report or more passively through a third-party subpoena or any investigative demand.

Companies should also be sensitive to increasing whistleblower activity. Current or former employees are incentivised to report potential misconduct to US regulators, which has led to substantial recoveries for the government. The SEC's whistleblower programme has been steadily active, with 67 individuals receiving approximately US$387 million between 2012 and November 2019. Whistleblowers are eligible to receive awards between 10 per cent and 30 per cent of the money recovered if their 'high-quality original information' leads to enforcement actions in which the SEC orders at least US$1 million.[42] The programme continues to be a priority for the Commission. In March 2018, the SEC announced its largest-ever whistleblower award, with two whistleblowers sharing nearly US$50 million and a third receiving more than US$33 million. In September 2018, the SEC awarded its second-highest whistleblower award of US$39 million to one whistleblower, with a second receiving US$15 million.[43] It is therefore important that a company consider the real possibility that its conduct could be exposed by means other than voluntary self-disclosure, and the associated, often expensive, risks associated with not being the first to come forward.

When deciding not to self-report, a company must ensure that the decision is appropriately considered and documented. If a company decides not to self-report and the government later enquires about the issue, the best defence is that the company conducted a thorough investigation, remediated the issue and had a reasonable basis for not self-reporting to the government. US regulators will look to a company's board of directors to ensure the appropriate steps were taken.[44] The SEC has expressed that the board of directors must exercise oversight and set a strong 'tone at the top' emphasising the importance of compliance.

42 More information is available at the SEC's 'Office of the Whistleblower' site at https://www.sec.gov/whistleblower.

43 See 'SEC Awards More Than $54 Million to Two Whistleblowers', available at https://www.sec.gov/news/press-release/2018-179.

44 Notification of the board of directors is often required under federal securities law. Section 307 of the Sarbanes-Oxley Act of 2002 requires that an attorney report evidence of a material violation of securities laws or breach of fiduciary duty by the company or any agent 'up-the-ladder' (i.e., first to the chief legal officer or CEO and, thereafter, if appropriate remedial measures are not taken, to the audit committee of the board or other board committee comprised solely of non-employee directors). Wherever possible, it is best to engage the board's disclosure counsel to assist in making this determination.

5

Beginning an Internal Investigation: The UK Perspective

Jonathan Cotton and Holly Ware[1]

Introduction 5.1

The trigger points for a potential internal investigation are increasingly diverse. Sources include employee allegations, whistleblowing, supplier or customer complaints, findings from internal or external audits, press reports, social media, blogs, third-party litigation and contact from government or regulatory authorities who may independently have uncovered an issue. In addition, potential issues may be uncovered during other internal investigations.

The focus of this chapter is on the key factors relevant to a company's decision whether, when and how to launch an internal investigation and to highlight key considerations when undertaking document preservation, collection and review. These decisions are often made under significant time pressure and with only limited information. They can, however, have serious repercussions.

Decision whether to notify any relevant authorities 5.2

A key initial question upon a potential issue coming to light is whether there is an obligation to notify any relevant authorities – which is likely, in turn, to impact the form of the internal investigation. Whether there is such an obligation will turn on the regulatory status of the company uncovering the issue, the expectations of the relevant authorities and the issue itself.

Firms regulated by the Financial Conduct Authority (FCA) are under a duty to deal with their regulators openly and co-operatively and to disclose appropriately

1 Jonathan Cotton and Holly Ware are partners at Slaughter and May. The authors would like to thank James Dobias for his assistance in preparing this chapter.

anything relating to them of which the FCA would reasonably expect notice.[2] The FCA Handbook sets out a non-exhaustive list of situations where a company is under an explicit notification duty, including where there has been a significant failure in the company's systems or controls, there has been a significant breach of a rule imposed by the FCA, employees may have committed significant fraud against customers, or a significant infringement of any applicable competition law has, or may have, occurred.[3] Although the timing of the notification will depend on the circumstances, the FCA expects a firm to discuss relevant matters with it 'at an early stage, before making any internal or external commitments' and in certain cases the notification obligation can be immediate.[4] Dual-regulated firms owe similar obligations to the Prudential Regulation Authority (PRA).[5]

Persons working in the 'regulated sector' (a wider concept than just firms regulated by the FCA) must submit (either directly or through their firm's nominated officer) a suspicious activity report (SAR) to the National Crime Agency (NCA) in respect of information that comes to them in the course of their business if they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, or even just attempting the latter.[6] Even if a person does not work in the 'regulated sector', they may still wish to make a voluntary SAR and an accompanying application for a 'defence against money laundering' if they suspect that property they are dealing with is in some way criminal, and that by dealing with it they risk committing a relevant money laundering offence.[7]

It may also be necessary to consider whether there are any notification requirements to professional bodies (e.g., the Solicitors Regulation Authority[8] or, for accountants, their applicable supervisory body[9]) or to the Information Commissioner's Office (for example if a personal data breach may have occurred).[10]

While there is no legal duty on a company to self-report to the Serious Fraud Office (SFO), the Deferred Prosecution Agreements Code of Practice (the DPA Code) states that it will be a public interest factor against prosecution if a company self-reports 'within a reasonable time of the offending coming to light';[11]

2 FCA Handbook, PRIN 2.1.1R, Principle 11. Relevant individuals are also subject to equivalent obligations under FCA Handbook, COCON 2.1.3 and COCON 2.2.4.

3 FCA Handbook, SUP 15.3.

4 Ibid.

5 PRA Rulebook, Notifications, Rule 2. (A dual-regulated firm is a firm that is a 'bank, a building society or a UK designated investment firm', FCA Handbook, SYSC 19 D.)

6 Sections 330 and 331 Proceeds of Crime Act 2002 and section 21A Terrorism Act 2000. 'Regulated sector' is defined in Schedule 9 of the Proceeds of Crime Act 2002.

7 Sections 335 and 338 Proceeds of Crime Act 2002.

8 See, for example, Rule 3 (Cooperation and Accountability), Code of Conduct for Firms, SRA Standards and Regulations.

9 For example, accountants regulated by the Institute of Chartered Accountants in England and Wales are subject to a reporting obligation under Disciplinary Bye-laws 9.1 and 9.2.

10 Article 33, General Data Protection Regulation 2016/679 (GDPR); section 67 Data Protection Act 2018.

11 Deferred Prosecution Agreements Code of Practice, paragraph 2.8.2(i).

a point that has been strongly endorsed by the courts in the DPA judgments handed down to date.[12] Likewise, in August 2019, the SFO published guidance on actions that companies being investigated by the SFO can take to increase their chances of earning 'co-operation credit' (Corporate Co-operation Guidance), which refers to reporting to the SFO 'within a reasonable time of the suspicions coming to light'.[13] This reference to 'reasonable time' allows some scope for a company to conduct at least a preliminary investigation into a potential issue prior to self-reporting, as reflected in a speech given by the current Director of the SFO, who acknowledged that companies 'have a duty to their shareholders to ensure allegations or suspicions are investigated, assessed and verified, so they understand what they may be reporting before they report it'.[14]

Decision whether and when to launch an internal investigation 5.3

In addition to considering whether and when to notify any relevant authorities, the company will also have to assess whether it would be in its interests to conduct an internal investigation. This is an important decision as, once begun, an internal investigation can be difficult to stop or limit without damaging the company's credibility.

There are, in general, a significant number of advantages to undertaking an internal investigation, including, principally, the ability to gain a better understanding of the facts to allow for more informed decision-making and the exploration of possible defences. There can also be significant financial benefits if the results of the investigation allow the company to apply for leniency or immunity (principally available in the competition sphere) or to self-report and co-operate with an external investigation to gain a discount on a potential future financial penalty (or avoid prosecution altogether). Undertaking an internal investigation can also help to show adequate procedures and a corporate culture where compliance is taken seriously, with wider benefits should the company's compliance framework later be assessed (whether in the context of this or another investigation). Linked to this, an internal investigation can also allow for proper remediation and the implementation of corporate changes that might help to avoid the issue arising in future. Electing not to investigate can mean a company is in a purely reactive position with regard to any parallel external investigation or news story.

In certain circumstances, the factors in favour of conducting an internal investigation can be particularly acute. This can include where a company is effectively required to investigate to comply with its regulatory obligations (for instance to

12 See, e.g., *Serious Fraud Office v. Standard Bank Plc (now known as ICBC Standard Bank Plc)* [2016] Lloyd's Rep FC 102, at paragraph 14, *Serious Fraud Office v. Tesco Stores Ltd* [2019] Lloyd's Rep FC 283, at paragraphs 66 and 117, and *Serious Fraud Office v. Serco Geografix Ltd* [2019] Lloyd's Rep FC 518, at paragraph 47.

13 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

14 Speech by Lisa Osofsky, Director, SFO, 3 April 2019, available at https://www.sfo.gov.uk/2019/04/03/fighting-fraud-and-corruption-in-a-shrinking-world/.

ensure compliance with the FCA Principles for Businesses)[15] or for directors to comply with their fiduciary and other statutory or common law duties.[16] A company may also have existing internal corporate governance codes or compliance policies that require an investigation to take place in the circumstances. On the other hand, in certain cases, authorities have been known to instruct companies not to conduct an internal investigation at all (for instance if it risks employees being 'tipped off' that they are under investigation, denying the authority the chance to monitor the relevant individuals covertly). Indeed, the FCA has stated that: 'Whether and how a firm investigates internally must now be looked at from the point of view of whether doing so will assist or inhibit the FCA's investigation.'[17]

There are, however, a number of potential downsides to conducting an internal investigation that in certain circumstances can allow a company to conclude not to investigate or to do so only in response to external requirements. These downsides include the potentially high costs and resource requirements of the investigation, the distraction from the day-to-day job, and the publicity and reputational risk that the investigation (should it be made public) might incur. Depending on the outcome of any investigation, companies may need to notify stakeholders (such as insurers, auditors, lenders – particularly where the facts may constitute an event of default – and affected third-party clients, customers and counterparties), and listed companies may be required to make a disclosure to the market. There is also the risk that the internal investigation might result in the creation of non-privileged documents that could assist regulators and prosecutors, as well as potential civil claimants (such as customers or shareholders), to the detriment of the company, or that the investigation might uncover misconduct beyond the scope of the initial allegation.

Alongside the decision whether and when to conduct an internal investigation is the decision whether to instruct external legal counsel to advise on or even conduct the internal investigation. In addition to providing investigations expertise and increased resources, the engagement of external counsel can also bolster the independence of the investigation, which is important in a criminal or regulatory context, and provide an external viewpoint to balance the views of internal stakeholders. External counsel also help to increase the likelihood that privilege may apply to certain investigation documents, especially where the in-house legal team that might otherwise be running the investigation hold dual business and legal functions.

15 FCA Handbook, PRIN 2.1.1R.

16 See, in particular, sections 171 to 177, Companies Act 2006.

17 Speech by Jamie Symington, then Director in Enforcement – Wholesale, Unauthorised Business and Intelligence, FCA, 5 November 2015, available at https://www.fca.org.uk/news/speeches/internal-investigations-firms. See also FCA Handbook, EG 3.11.7.

Oversight and management of the investigation 5.4

On taking the decision to undertake an internal investigation, a threshold issue to determine will be the governance structure for the investigation, including who will have day-to-day management of the investigation and whom they will report to. The structure chosen will vary depending on the company and the issue.

It is common for responsibility for day-to-day management of the investigation to be given to the internal legal or compliance team, although alternatives include oversight by the board as a whole, the audit committee or a specially constituted board subcommittee. The chosen entity would likely also be the 'client' for the purposes of instructing external legal counsel, with a consequent effect on the analysis of when legal advice and litigation privilege may arise. In any case, it will be important for potentially implicated individuals to be excluded from the investigation team, which should be kept under review in case additional individuals are implicated during the investigation. Further, where external advisers have been brought in to conduct an independent review, to preserve this independence, it may be necessary to limit the ability of the client to instruct or influence the review beyond clearly defined parameters.

See Chapter 35 on privilege

The question of whom the investigation team will report to will often be determined by a company's existing corporate governance structure and framework of delegated authorities. However, in certain cases the company may choose to constitute a specific review body, such as a special subcommittee of the board or a panel of senior employees and external advisers. In such cases, the terms of reference of this body will need to be clearly defined, including what matters are to be referred to it, what powers it holds and how it is to interact with existing governance bodies in the company.

Where, as is common, the issue involves subsidiaries (some of which may not be wholly owned), it may be necessary to include considerations as to corporate separateness in the governance structure, including the possible need to report to the boards of these subsidiaries.

Whatever governance structures are selected, it will be important to keep these under review and be flexible as to potential amendments to reflect the changing scope of the investigation as new issues arise.

Determining the internal investigation's scope 5.5

Having a clearly defined scope, as reflected in written terms of reference and an investigation plan, is important to set clear objectives and the steps to help avoid a wide-ranging, unfocused investigation, with consequent wastage of time, resources and cost. Clearly setting and justifying the scope will also better allow the investigation to be auditable if queries arise in the future.

See Section 5.6.5

A number of variables will feed into the decision on scope, and there is no one-size-fits-all solution. A narrow scope can help to focus resources and reach a quicker conclusion, but it may risk missing potential conduct or valuable context. A wider scope can help to demonstrate that the investigation has been comprehensive, but it can be expensive and slow. In any case, the scope will be affected by the issues (including whether the company is facing criminal, regulatory or

civil claims risk), the time pressures (especially if the company is in a race against co-infringers to apply for leniency) and whether there are concurrent investigations by authorities or internal investigations in other jurisdictions.

Part of defining the scope will also include a decision as to the final deliverables. While the default may be the production of a factual summary report alongside legal advice as to the company's exposure, there is a risk the former may not be privileged. An alternative is for the investigation team to provide only oral updates on the factual findings. Other deliverables can include advice on potential self-reporting, employment law advice on disciplinary action against implicated employees, and proposals as to mitigation and remediation activities to help ensure the conduct is not repeated. The FCA Handbook states that a firm's willingness to volunteer the results of its own investigation, whether protected by legal privilege or otherwise, is welcomed by the FCA and is something the FCA may take into account when deciding what action to take.[18] Likewise, the DPA Code notes that co-operation (which is a public interest factor against prosecution) will include a company sharing its internal investigation report (including source documents) with the SFO; a point which has been highlighted by the courts in the DPA judgments handed down to date.[19]

Companies must also assess whether the scope and terms of reference need to be agreed in advance with any authorities that are aware of the issue to be investigated. The benefits of doing so include potentially building co-operation credit with the authorities, reducing the risk of the authorities later criticising the scope of the investigation and allowing the authorities an opportunity to express their preferences as to the final deliverables and the practical conduct of the investigation. The SFO has been particularly concerned about the potential for internal investigations to 'trample over the crime scene', and early engagement can help to avoid later criticism of the investigation team's actions.[20] Further, the FCA Handbook states that if a firm anticipates that it will disclose a report of its internal investigation to the FCA, the potential use and benefit to be derived from the report will be greater if the FCA has had the chance to comment on its proposed scope and purpose.[21]

Finally, at the scoping stage it can be helpful to assess what external resources may be required during the investigation, including the potential use of forensic accountants, asset tracers, private investigators, third-party experts, public relations firms, and local and foreign counsel.

18 FCA Handbook, EG 3.11.2.

19 Deferred Prosecution Agreements Code of Practice, paragraph 2.8.2(i). Also see *Serious Fraud Office v. Rolls-Royce Plc and Another* [2017] Lloyd's Rep FC 249, at paragraph 17, and *Serious Fraud Office v. Serco Geografix Ltd* [2019] Lloyd's Rep FC 518, at paragraph 24.

20 Speech by Ben Morgan, then Joint Head of Bribery and Corruption, SFO, 20 May 2015, available at https://www.sfo.gov.uk/2015/05/20/compliance-and-cooperation/.

21 FCA Handbook, EG 3.11.5.

Document preservation, collection and review 5.6

In any internal investigation, it is critical to consider at the earliest possible opportunity the practicalities for the preservation, collection, review and analysis of relevant material. In its Corporate Co-operation Guidance, the SFO states that co-operation includes preserving available evidence and producing it to the SFO in an 'evidentially sound' format.[22] Any decisions should then be recorded in a written investigation plan to preserve a clear audit or 'chain of custody' trail. See Section 5.6.5

Although in the early stages of an investigation it may not be appropriate to conduct formal interviews, the investigation team may wish to consider conducting informal 'scoping interviews' to assist with scoping out the issues and identifying where relevant material might be stored. Care will need to be taken, given the preference of a number of authorities that they be consulted prior to interviews (even those relating to the location of evidence) to avoid the possibility of the internal investigation tainting the recollection of witnesses.

Preservation 5.6.1

An important first step in document preservation is to identify who might hold information relevant to the investigation. The pool of people is likely to be broader than just those implicated in the conduct and may also include individuals reporting to them, individuals to whom they reported, secretaries and assistants, individuals in other departments they interacted with, and third parties outside the organisation. In some investigations, wider business units or offices might also be relevant.

In general, a company would then issue a hold notice (also known as a document retention or document preservation notice) to such individuals asking them to preserve (and not alter, discard, delete or destroy) all materials (including hard-copy materials) they may hold relevant to the investigation. Beforehand, however, the company should consider whether circulation of the hold notice may risk tipping off individuals relevant to the investigation if there is a risk they may destroy documentation or otherwise frustrate the investigation. In its Corporate Co-operation Guidance, the SFO states that genuine co-operation is inconsistent with 'putting subjects on notice and creating a danger of tampering with evidence or testimony'.[23] Potential solutions to address this risk include delaying the circulation of the hold notice until relevant materials have already been secured or carefully drafting the content of the hold notice so that it does not necessarily reveal the specific circumstances or content of the internal investigation (subject, however, to the data privacy considerations discussed below). The company should also consider the risk of a possible leak and whether the description in the hold notice may go beyond relevant market disclosures.

Companies should take care to keep a clear record of the recipients of these hold notices, especially where they are not circulated centrally, but instead are

22 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

23 Ibid.

cascaded via the reporting structures of the organisation. As part of this, companies may wish to ask employees to acknowledge their receipt and understanding of the hold notice, though this can create an administrative burden and raises the possibility that an employee may refuse to acknowledge receipt. A middle ground may involve requesting an email read-receipt instead.

In support of the hold notices (which are issued to, and place the burden of preservation on, the relevant individuals), companies should also consider implementing background procedural steps to help ensure the preservation of relevant data. This can include the suspension of regular document destruction processes, activating permanent email holds (so that individuals cannot permanently delete data from their inbox), retaining computer drive backups (so that if individuals delete data from a shared drive, it can be recovered), retaining employee devices and preventing the recall of documents from archives without appropriate authorisation. It is good practice to implement these before the circulation of the hold notice to reduce the risk of individuals deleting data.

Preservation also requires companies to be alert to the risk of ageing technology or bespoke systems and to take steps to ensure that the data stored within them remains accessible during the investigation.

When issuing hold notices or implementing procedural steps to help ensure the preservation of relevant data, companies should carefully consider the potential application of data privacy rules and appropriately document their consideration of the data subjects' interests. In particular, key considerations under the General Data Protection Regulation (GDPR) would include ensuring appropriate transparency (so that the data subjects are aware of the scope and purposes of the preservation), data minimisation (so that no more data is preserved than is necessary) and storage limitation (so that the data is not stored for longer than is necessary).

See Chapter 40 on data protection

5.6.2 Collection

Having preserved all relevant data, the next step is to identify what should be extracted and made available for potential review. A key part of this involves identifying which individuals are most likely to hold data relevant to the investigation (referred to as 'custodians') and which other sources might yield relevant documents (including any third-party sources). Companies will also need to identify what categories of material to collect, with a non-exhaustive list of options including emails, electronic documents, external storage devices, mobile phones, tablets, internet messaging and chatroom data, telephone recordings[24] and hard-copy materials.

Companies should also identify any material they are unable to access (such as private email accounts, messaging applications or social media) as the relevant authorities may have statutory powers that allow them to access these sources.

24 The FCA Handbook (SYSC 10A.1) places obligations on regulated firms to record telephone conversations that relate to regulated activities in certain financial instruments.

In its Corporate Co-operation Guidance, the SFO has stated it will consider it a mark of co-operation for companies to alert the SFO if there are any such inaccessible sources.[25]

Depending on the circumstances of the investigation, it may be desirable to instruct an external forensic provider to undertake the data collection. This will be especially important in the criminal context where issues relating to the forensic integrity of the underlying data and chain of custody are key.

When undertaking the collection, the decision will need to be taken whether the affected individuals should be notified. Relevant factors include the terms of any applicable data privacy policies at the company (including the existing description of the purposes for which the company might process the individuals' data) and the likelihood that giving notice may result in individuals destroying documents or otherwise frustrating the investigation. In certain circumstances, express consent may be required from employees, especially if required by local data privacy laws or if the employees use their own devices.

When undertaking the collection, it will also be necessary to consider the requirements of applicable data privacy rules more generally. Considerations as to data minimisation can require the collection to be limited by date range and search terms (even before the data is ingested into a review platform) and the principles of integrity and confidentiality require the data to be stored securely and only accessible with appropriate authorisation.

See Chapter 40 on data protection

For both preservation and collection, it will be necessary to record all steps taken and keep any decisions under review as the investigation identifies new custodians, sources and date ranges.

Review 5.6.3

Having collected the data, in all but the smallest reviews, it is advisable to upload it to a document review platform. This allows for easier searching, tagging and management of the data and will create an audit trail if questions arise in relation to specific documents.

The next stage will be to assess the appropriate searching criteria to help narrow the scope of the review and identify the most relevant documents. Tools here include applying date range, custodian and data source filters and identifying relevant search terms. If the timing allows, there are significant benefits to testing the potential searching criteria and refining them before starting the full review. A clear record should be kept of all decisions taken, including the reasons for refining or abandoning any provisional search criteria. There are also significant benefits to considering the appropriate type of data de-duplication to conduct.

Increasingly, many vendors are offering technology-assisted analytics and technology-assisted review (TAR), which allow for the review platform to learn from initial reviewer coding decisions and identify similarly relevant documents from the remaining data set. This can allow the technology to prioritise these

25 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

documents, ensuring they are brought to the attention of the review team sooner, or even automatically code the documents. The success of this technology will, however, depend significantly on the quality of the initial 'seed set' of coding decisions and the complexity of the issues it is being asked to assess.

In any case, it is common to structure the review around a series of 'tiers', with an initial triage stage for relevancy, followed by second and potentially third-tier reviews by more senior individuals to focus the set and apply more complex coding. In a number of cases, first-tier and even second-tier reviews are outsourced to specialist external document review teams, which can free resource within the investigation team to concentrate on management of the review and the other elements of the investigation.

To ensure accuracy and consistency of coding, it will be necessary to draft document review protocols and accompanying coding forms for each tier of the review, together with organising training for the reviewers. It is also common to organise regular quality control or calibration sessions with the reviewers, where they can ask questions of the senior team, and to set up a process for the rapid escalation to the senior team of key documents identified during the review.

In drafting the document review protocol and coding forms, it will be important to consider how the internal review may interact with any existing or potential parallel external investigation. In particular, if there is the possibility that relevant documents may be produced to an authority, there may be benefits at this stage to asking reviewers to code for privilege, data privacy, bank confidentiality and other jurisdiction-specific issues.

5.6.4 Data located in multiple jurisdictions

Particular complexities can arise where data relevant to the internal investigation is located in other jurisdictions (including where it is hosted on cloud-based or group-wide servers that might be physically located overseas).

It will often be necessary to get local data privacy advice before preserving and collecting data for review, including on whether and how the data may be transferred to the jurisdiction where the review is taking place. If transfer of the data is not permissible, it may be necessary to conduct a local review within the foreign jurisdiction.

There are also wider strategic considerations to bear in mind before deciding to collect and transfer data from other jurisdictions. In particular, consideration should be given to the risk of transferring documents into a jurisdiction where they might not otherwise have been available to authorities or to claimants during disclosure in civil trials (although this should be balanced against the risk that in not collecting this data the company may be found to be non-co-operative or frustrating the investigation).[26] Likewise, where the data is held by a subsidiary,

26 It is possible for authorities in one jurisdiction to request documents from authorities in other jurisdictions via diplomatic channels, including via mutual legal assistance treaties. In addition, in February 2019, the UK government introduced the Crime (Overseas Production Orders) Act 2019, which aims to simplify and speed up obtaining electronic data located abroad.

considerations as to corporate separateness may require the two companies to enter into co-operation and information sharing agreements with respect to the investigation. It is common in these agreements (especially where the subsidiary is not wholly owned) for the subsidiary to retain a right of consent prior to its data being disclosed to any authority.

The UK authorities tend to be more willing than their US counterparts to engage with companies' representations as to limitations imposed by overseas jurisdictions. A risk remains, however, that in failing to collect, transfer and review relevant data, a company may be found to be non-co-operative or obstructive of the authorities' investigations.

Importance of record-keeping 5.6.5

As referenced above, it is critical at all stages of an internal investigation to keep clear records of key decisions taken, including the drafting of detailed, auditable summaries of the methodology undertaken for data preservation, collection and review. It will also be important to preserve originals of all relevant documents and devices and maintain a full chain of custody records.

The FCA Handbook states that where a firm conducts an internal investigation, it will be 'very helpful' if the firm maintains a proper record of the enquiries made and interviews conducted.[27] Likewise, in its Corporate Co-operation Guidance, the SFO has emphasised the importance of maintaining an audit trail of the acquisition and handling of digital, hard-copy and financial material, and the potential need for companies to identify a person to provide a witness statement covering such issues.[28]

27 FCA Handbook, EG 3.11.9.

28 SFO Operational Handbook, Corporate Co-operation Guidance, August 2019.

6

Beginning an Internal Investigation: The US Perspective

Bruce E Yannett and David Sarratt[1]

6.1 Introduction

The aim of this chapter is to provide the reader with useful tools to navigate the beginning of an internal investigation. Mistakes made in the initial phases of an investigation can have costly repercussions down the road, and, for this reason, it is important to consider all the relevant legal, commercial and logistical factors in making strategic decisions early on.

6.2 Assessing if an internal investigation is necessary

Information giving rise to the need for an internal investigation can come from a variety of sources, including customers, employees, whistleblowers, lawsuits, counterparties, news and social media, as well as from prosecutorial and regulatory authorities. Regulatory changes have created new incentives for individuals to come forward and report suspected wrongdoing. For example, the Sarbanes-Oxley Act of 2002 and its implementing rules require attorneys who appear and practise before the SEC to report evidence of a material violation up the ladder to a company's chief legal officer and CEO. The reporting obligation is not discharged until the attorney reasonably believes the company has provided an appropriate response.[2] Similar reporting obligations apply to issuers and auditors.[3]

When confronted with information – from whatever source – that the company or its employees may have engaged in serious misconduct, in-house counsel's first step is often to assess whether it would be in the company's interest to conduct an internal investigation. Counsel will want to consider whether

1 Bruce E Yannett and David Sarratt are partners at Debevoise & Plimpton LLP.

2 See Sarbanes-Oxley Act of 2002 § 307, 15 U.S.C.A. § 7245 (2002); 17 C.F.R. Part 205.3(d).

3 See Securities Exchange Act of 1934 § 10A, 15 U.S.C.A. § 78j-1.

government authorities are already investigating, or are likely to investigate, the matter, whether civil litigation will follow and in what form, and the potential (or likely) need for remediation. Depending on the facts, counsel may also want to balance the costs of investigating and the potential disruption to normal business, as well as any potential reputational risk or commercial fallout.

In some instances, external legal obligations may require an investigation to be conducted. Board members and management, for example, have a fiduciary duty to protect the interests of the corporation and its shareholders, and in some cases that duty will include an obligation to investigate indications of serious misconduct at the company. An investigation may also be required in certain instances so that company executives can meet any affirmative certification obligations they have, whether under Sarbanes-Oxley or otherwise.

More often, however, counsel will want to conduct an investigation to make an informed decision about whether it is in the company's interest to self-report the matter to law enforcement or regulators. Over the past two decades, the United States Department of Justice (DOJ) has placed an increasing focus on self-reporting both in charging decisions and in the degree of co-operation credit that will be afforded to a company. To guide the charging decisions of its own attorneys, the DOJ has set out a number of factors that prosecutors should consider in determining whether to charge a business entity, including co-operation and voluntary disclosure, the adequacy of the corporation's compliance programmes, and any remedial actions or restitution undertaken.[4] The DOJ has expanded on these factors through subsequent directives.[5] Most recently, in November 2019, the DOJ clarified that under its revised policy, a company seeking co-operation credit is expected to disclose 'all relevant facts known to it at the time of the disclosure, including as to any individuals substantially involved' in the misconduct. This clarification recognises that because 'a company may not be in a position to know all relevant facts at the time of a voluntary self-disclosure, especially where only preliminary investigative efforts have been possible', a full investigation is not required before disclosure, though a company should 'provide a fulsome disclosure' of the relevant facts known at the time.[6] Additionally, in 2016, the Fraud Section of the

See Chapter 4 on self-reporting to authorities

4 See Holder Memorandum, Bringing Criminal Charges Against Corporations, Dep't of Justice, Deputy Attorney General Eric Holder (16 June 1999).

5 See Thompson Memorandum, Principles of Federal Prosecution of Business Organizations, Dep't of Justice, Deputy Attorney General Larry D Thompson (20 January 2003); McCallum Memorandum, Waiver of Corporate Attorney–client and Work Product Protections, Dep't of Justice, Acting Deputy Attorney General Robert D McCallum (21 October 2005); McNulty Memorandum, Principles of Federal Prosecution of Business Organizations, Dep't of Justice, Deputy Attorney General Paul J McNulty (12 December 2006); Filip Memorandum, Principles of Federal Prosecution of Business Organizations, Dep't of Justice, Deputy Attorney General Mark Filip (28 August 2008); Yates Memorandum, Individual Accountability for Corporate Wrongdoing, Dep't of Justice, Deputy Attorney General Sally Q Yates (9 September 2015).

6 United States Department of Justice, Justice Manual § 9-47.120 (updated November 2019). The revised policy also provides that a company must let the DOJ know 'where the company is aware of relevant evidence not in the company's possession'.

DOJ launched a 'Pilot Program' announcing even greater emphasis on voluntary self-reporting in deciding whether to charge or how to resolve corporate criminal matters.[7] The following year, this policy was formally implemented through the DOJ's revised Policy on Corporate Enforcement of the Foreign Corrupt Practices Act, which was announced on 29 November 2017 and closely tracks the objectives of the Pilot Program, including the incentives for self-disclosure and co-operation with the DOJ's investigations.[8] The DOJ has since indicated that this policy will likely be extended, at least in practice, to cases that come before the Department involving other federal regulations beyond the FCPA.[9]

In light of these policies, for all practical purposes, an internal investigation is often necessary so that the company can identify what, if any, information should be disclosed to the DOJ, and whether co-operation credit is attainable. This, however, may be a false dilemma as, in many instances, a corporation's co-operation can be the most significant determining factor in how the DOJ resolves a case, including the amount of any penalty.[10]

Many regulatory agencies have likewise increasingly come to expect companies to perform a robust internal investigation of any potential legal or regulatory violations and to report such violations to the agency. For example, the Consumer Financial Protection Bureau (CFPB) has stated that 'responsible conduct' – namely proactive self-policing for potential violations, prompt self-reporting of identified violations, complete remediation of resulting harm and co-operation with the CFPB – would influence the CFPB's resolution of an enforcement investigation.[11] Similarly, the US Department of Treasury Office of Foreign Assets Control specifically provides companies with mitigation credit of 50 per cent off its base penalty amounts for voluntary disclosures and further mitigation for co-operation.[12] The SEC similarly identifies '[s]elf-policing, self-reporting, remediation and cooperation with law enforcement authorities' as the primary factors it will consider in determining an appropriate resolution.[13]

---

7 Leslie R Caldwell, Criminal Division Launches New FCPA Pilot Program (5 April 2016) (noting that '[i]f a company opts not to self-disclose, it should do so understanding that in any eventual investigation that decision will result in a significantly different outcome than if the company had voluntarily disclosed the conduct to us.').

8 See Deputy Attorney General Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices Act, U.S. Dep't of Justice (29 November 2017); U.S. Dep't of Justice, Justice Manual § 9-47.120 (updated November 2019).

9 See Head of the Criminal Division John Cronan and Chief of the Securities and Financial Fraud Unit Benjamin Singer Deliver Remarks at the ABA's 32nd Annual National Institute on White Collar Crime (1 March 2018); Letter Declining to Prosecute Barclays PLC (28 February 2018), stating: 'The Department's decision to close its investigation of this matter is based on a number of factors, including . . . Barclays' timely, voluntary self-disclosure.'.

10 U.S.S.G. § 8C2.5(g), cmt. 13 (2015).

11 CFPB Bulletin 2013-06, Responsible Business Conduct (25 June 2013).

12 31 C.F.R. Part 501, Economic Sanctions Enforcement Guidelines (9 November 2009).

13 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Release No. 34-44969 (23 October 2001) (Seaboard Report).

Even apart from legal considerations, business and reputational concerns alone may provide grounds for conducting an internal investigation. Indeed, counsel will often need to have a baseline understanding of the underlying facts, and an informed sense of whether there is any substance to the allegations of misconduct, to make a reasonable assessment of the potential business and legal consequences and the need for corrective action. Commencing a thorough internal inquiry will often also be important to any related public relations efforts, and will be critical to maintaining the company's credibility with its customers, business partners and other affected individuals.[14]

Identifying the client 6.3

Once the company decides to commence an internal investigation, the next step is to determine who will conduct the investigation and for what specific client within the organisation. In large organisations, particularly those with multiple subsidiaries across the globe, counsel should think strategically about how to structure the investigation: where to locate the attorney–client relationship, to whom the investigating attorneys should report, and who will be making key decisions as the investigation proceeds. In making these decisions, counsel should consider what relationships will best protect the integrity and confidentiality of the investigation, the location and custody of relevant documents, and the overall aims of the investigation over the short and long term.

In some circumstances, counsel may also want to consider whether the investigation should be conducted on behalf of the board (or its subcommittee), with counsel reporting to and being directed by the board, rather than management. In a shareholder derivative suit, having the board direct the investigation will be the norm, both because the conduct of management will often be at issue and so that the investigation will not be subject to the derivative-claim exception to the attorney–client privilege recognised in some jurisdictions. The board may also be best suited to lead an investigation when the allegations are particularly serious or could have serious consequences for the company, when the allegations concern the actions of senior management, or when reputational or other concerns require that the investigation be conducted independently of management. Making that decision in any particular case will depend heavily on the specific facts involved, the company's business and position in the marketplace, the relationship dynamics at the company and the overall goals of the investigation.

See Chapter 36 on privilege

Whatever decision is made, it is important that the company clearly document who the client is, and the reporting and oversight structure for the investigation.

14 In rare circumstances, some facts will be so clearly unlawful on their face (e.g., if an employee is providing clearly and materially false information to investors) that the company should consider notifying the relevant law enforcement or regulatory authorities even before conducting a complete internal investigation, particularly where time is of the essence and, if appropriate, continue with the internal investigation in parallel.

6.4 Control of the investigation: in-house or external counsel

Although routine matters can often be handled by in-house counsel, an outside firm should ordinarily conduct the investigation where the potential misconduct could produce significant adverse legal or commercial consequences for the company. Though internal investigations can be expensive and time-consuming, these concerns often pale in comparison to the possible legal, financial and reputational risks faced by the company, as well as the need to demonstrate independence. Hiring external counsel allows for a clearer application of attorney–client privilege to the communications and work-product of the outside firm, especially where corporation counsel has both business and legal functions. Often, both commercial and legal concerns can precipitate an internal investigation, so using external counsel can decrease the risk of inadvertently waiving privilege.[15] External counsel also brings expertise, experience and resources to support the company in challenging situations that are unlikely to arise with much frequency at any particular company.

Depending on the circumstances, in-house counsel may want to consider using external counsel that is not the company's usual firm.[16] Bringing in a separate firm that is less familiar with the company's business, of course, will often involve additional time and expense. Whether this step is justified in a particular case will depend on the sensitivity and significance of the investigation, the level of management implicated in the conduct, the need for perceived independence of the investigation, and the attitude of potentially relevant regulators who may be assessing the quality and results of the investigation in considering whether the company deserves credit for co-operation.

6.5 Determining the scope of the investigation

The importance of clarifying the investigation's scope and purpose at the outset cannot be overstated. First, a well-defined and memorialised purpose can help establish the legitimacy of privilege claims over attorney–client communications and work-product produced in the course of the investigation; the claim to attorney–client privilege is likely to be much stronger if an independent investigation has been commenced or litigation is reasonably in contemplation.

See Chapter 36 on privilege

Additionally, defining the investigation's purpose can impose a welcome discipline and accountability on the investigators themselves. Corporate counsel are

15 See, e.g., *United States v. Ruehle*, 583 F.3d 600, 606-12 (9th Cir. 2009) (statements made for the purpose of disclosure to outside auditors not privileged). In the United States, however, investigations conducted solely by in-house counsel may fall within the scope of attorney–client privilege if they are carefully conducted. See, e.g., *In re Kellogg, Brown & Root, Inc. et al.*, 756 F.3d 754, 758 (D.C. Cir. 2014) ('*Upjohn* does not hold or imply that the involvement of outside counsel is a necessary predicate for the privilege to apply.'). The extent to which an investigation conducted by in-house counsel outside the United States would be protected by privilege varies widely by jurisdiction.

16 See *In re John Doe Corp.*, 675 F.2d 482, 491 (2d Cir. 1982) (recognising that when corporate counsel finds evidence of criminality protected under *Upjohn* 'the wiser course may be to hire counsel with no other connection to the corporation to conduct investigations').

quite familiar with the tangents that can cause an investigation to become rudderless and wasteful. As explained below, a short period of preliminary investigation can often be helpful in defining a purpose and scope to the investigation that is reasonably clear and realistic, while identifying key uncertainties and inflection points to come. In defining the scope of the investigation, it can also be valuable to consider how quickly the information is needed, whether based on requests from the government or internal time pressures.

Key documents and scoping interviews 6.5.1

Most investigations will begin with counsel's review of a handful of critical documents that are at the heart of the information triggering the need for the investigation. In many instances, the documents themselves, rather than individuals, may have alerted the company to alleged wrongdoing and precipitated the need for an investigation. In almost every case, however, conducting a small number of initial scoping interviews will be a useful way for the investigators to focus in quickly on the truly important material.

Identifying the most useful individuals to speak with in these scoping conversations can be delicate, as investigators seek to strike a balance between speaking with individuals who are knowledgeable about the issue at hand but who are sufficiently removed from the potential misconduct that they can safely be viewed as reliable in terms of setting the scope and maintaining the confidentiality of the investigation. Of course, interviewing an employee at an early stage, without the benefit of a complete set facts or documents, could result in incomplete information and the need for a further interview.

One logical place for external counsel to start is to thoroughly debrief the in-house legal team and, potentially, the individual or individuals who brought the issue to the attention of the organisation. These interviews can serve to identify key custodians, the nature and volume of relevant documents, the ways documents are stored, and who has access to them. If there is an obvious investigation target, interviewing that individual in the initial stages may be more efficient, but this must be weighed against other strategic considerations, including alerting the target to the focus of the investigation and compromising the investigation later on. The timing and structure of these initial discussions may also be influenced by external deadlines or other business considerations involved in the review.

Identifying necessary partners 6.5.2

Another early consideration for counsel is what outside investigative partners may be needed. These can range from technical subject-matter experts to local counsel in foreign jurisdictions to data processing and hosting services to forensic accountants. Counsel ordinarily will want to interview a number of firms in deciding which vendors to use, and the discussions can sometimes yield helpful insight into the size of the tasks ahead, likely costs, potential alternative strategies and timing. Engaging these third parties at the outset of the investigation – even if their work is not needed immediately – will often be valuable in defining the scope and methods of the investigation. As noted above, given the consideration

of attorney–client privilege, generally external counsel will retain the third-party vendors on behalf of the company so that their work and work-product is undertaken on the instruction of external counsel in anticipation of litigation and thereby covered by privilege and attorney work-product protections.

6.5.3 Developing a work plan

Once the investigating attorney has identified the subject matter of the investigation (the who, what, when and where), the scope and the purpose of the investigation and a concrete plan for carrying it out should ordinarily be memorialised by external counsel in a written work plan. This type of memorandum allows for client input on the investigative process, gives in-house counsel clear expectations about how the investigation will progress, and provides investigating attorneys with a benchmark for strategic judgements as the investigation moves forward. It can also serve as a useful tool for dividing responsibilities among the investigating attorneys and tracking progress toward key investigative goals. Keep in mind that the work plan may be a document that the company decides to share with the criminal or regulatory authorities and should be drafted accordingly.

In building the work plan, counsel should consider the time frame and geographical range of the inquiry, as well as which entities of the company (e.g., subsidiaries, affiliates, departments) will be covered and, if applicable, the rationale for not covering other entities at this stage. The memorandum should clearly set forth the subject matter under investigation and, to the extent possible, (1) what company documents will be retrieved (and by whom), (2) how data will be processed (and by whom), and (3) how documents will be reviewed (and by whom). In collecting, reviewing and preserving documents, the investigating attorney should take into account any data privacy concerns that may arise.

See Section 6.6.2

Where possible, the work plan should list any interviews that have been or will be conducted, or at least the categories of people to be interviewed. To the extent there is a rationale for interviewing some individuals and not others, it should be stated. Likewise, if the involvement of other third parties, such as forensic accountants and industry experts, is foreseeable, the document should describe the scope of their expected engagement.

The work plan should also set a rough schedule for key deliverables in the investigation, and at least tentatively identify the form that the ultimate work-product will take. In particular, it is useful to know at the outset of an investigation whether the preparation of a written investigative report will be useful and in the company's interest, or whether an oral presentation of findings to management or the board would be preferable. A written report will most often be advisable when the company believes providing the report to a third party or to the public will be beneficial, whether for reputational, business or legal reasons. In most other cases, an oral report will often serve the client's interests just as well without creating a risk of inadvertent or compelled disclosure.

Finally, the work plan should be flexible. Although careful planning is always beneficial, investigations in the real world are not scripted affairs. The investigative team will have to adapt to new information and challenges as the investigation

progresses, and the work plan should lay out a process for making those decisions – particularly in terms of who should be consulted and who should approve – before the investigative team moves in a new direction not contemplated by the plan.

Certain investigations may implicate the general counsel or other members of senior management in alleged misconduct. In that circumstance, the investigating attorneys should report to the board (or a designated member or committee of the board) or to a senior executive who has no involvement in the facts at issue and who does not report to any member of management whose conduct may be under review.

Document preservation, collection and review 6.6

Preservation 6.6.1

As soon as possible after learning of potential misconduct, the in-house attorney should implement a litigation hold and document preservation notice to prevent the intentional or inadvertent destruction of relevant documents and material. In fashioning the document retention policy, it is ordinarily advisable to err on the side of overbreadth, at least at the beginning when the extent of any potential wrongdoing and the relevant actors are unknown. This is critical. Failure to successfully preserve relevant material could be viewed as a dereliction of the attorney's duties and, in some cases, as obstruction of justice.

In issuing preservation or 'hold' notices, the investigating attorneys should consider who should receive these notices (including the IT and records departments), what types of documents and data should be included, and how the investigation should be described. Where notices are sent to different jurisdictions, the investigating attorney may need to consider providing translations as well as addressing data privacy restrictions. The attorney implementing the litigation hold should record the distribution of notices and, where extra caution is warranted, have employees sign and return a copy of the notice or electronically acknowledge receipt so as to create a record. If the company has received a subpoena from law enforcement relating to the subject matter of the investigation, the subpoena will define the minimum universe of documents that require preservation, but counsel should consider whether additional material should be preserved for purposes of the internal investigation or otherwise.

See Section 6.7

The investigating attorneys should consult with the company's records management department to preserve any hard-copy files, including those stored off-site in archives. The investigating attorney should also instruct the IT department to suspend any normal data destruction practices and to create and maintain a list of the relevant sources of data. Such sources may include documents maintained on the company's servers and employees' hard drives, emails saved on exchange servers, data held on employees' home computers, and data saved on employees' work-issued mobile devices. In recent years, regulators have been increasingly focused, not just on collecting and preserving email, but also on collecting and preserving text messages and other communications stored on mobile and other

electronic devices.[17] To the greatest extent possible, the company should take steps on its own to preserve this electronic data rather than relying on individual employees to preserve their own documents. The company should also take steps to prevent individuals from destroying or altering potentially relevant data. In some cases the facts will warrant proactive data capturing steps, including forensic images of employee laptops, desktops or mobile devices. Document custodians should be designated as soon as the investigating attorneys reasonably believe such individuals may possess documents relevant to the investigation.

It bears mention that sometimes the document collection process itself can come under scrutiny, particularly if authorities come to believe that relevant (and potentially damaging) documents may have been destroyed. In some extreme cases, someone with first-hand knowledge of the investigation may be called to provide sworn testimony in a deposition or in court. Attorneys should plan and document the collection process with this worst-case scenario in mind, and make clear to their clients the importance of treating the collection process – sometimes viewed as a ministerial chore – with serious care and attention.

6.6.2 Collection

Once preservation measures have been implemented, the investigation can turn its attention to the collection of documents. Almost all investigations require judgement calls to be made on the scope of which documents to collect and from whom, including whether the investigation can be accomplished in whole or in part through collection within the company or, instead, requires collection from third parties. Company policies (e.g., codes of conduct) and local employment law also may impose limitations on the collection process. If the investigation contemplates the collection of personal health information, counsel should ensure that all data collection comports with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In such circumstances, counsel should take appropriate measures to safeguard personal health data, including assessing whether entering into a business associate contract is appropriate.[18] By the same token, counsel should ensure that any other personally identifiable information (PII) collected as part of the investigation is similarly flagged during review and appropriately safeguarded.

For electronic data, the process of collecting data will often coincide with preserving it. Counsel should make sure that forensic copies of all relevant electronic data (including metadata) has been copied to a secure location, preferably with

17 For example, for a company to receive full credit for timely and appropriate remediation in FCPA matters, the DOJ expects companies to implement 'appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations.' U.S. Department of Justice, Justice Manual § 9-47.120 (updated November 2019).

18 The HIPAA Rules generally require that covered entities enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. See 45 C.F.R. Part 160 and Part 164.

at least one backup maintained on a separate system. The data will then need to be loaded into a review platform for review. Evidence that has been collected in paper form will often be most easily reviewed by digitising it and loading it into the same review platform as the electronic documents that have been collected. The data vendor retained by the investigating counsel will provide the collection and hosting support to the company.

As with the preservation process, the steps taken in collecting documents should be recorded. In instances where requested documents cannot be located, the search efforts and results should also be documented.

Review 6.6.3

Regarding the review of the documents, the investigating attorneys should carefully consider how best to manage the volume and formatting of documents. Outside vendors are a useful resource for these matters, and consulting with them early can often save time and money.

Where there is a large volume of documents to be searched, the key objective is to locate the responsive documents quickly and efficiently. Search terms should be broad enough to include responsive materials, but narrow enough not to bog down review teams with a large proportion of unnecessary documents. To the extent certain custodians or groups of documents are more likely to contain relevant content, their review should be prioritised.

In recent years, great advances have been made in the use of predictive coding in e-discovery to more quickly identify relevant documents and reduce the number of non-responsive documents that need to be individually reviewed. In our experience, the judicious use of predictive coding technologies is increasingly acceptable to regulators and prosecutors in the right context, so long as the specific methodologies and rationale for using those tools are clearly discussed with the authorities at the outset. Even in cases where a full human review of a document population is contemplated or required, predictive coding can be a useful tool for internal investigators in locating the most relevant documents quickly, before the full review is complete.

Taking these considerations into account, the investigating attorneys should draft a document review protocol that sets forth in as much detail as possible the purpose of the review, the responsive issues, and how documents should be tagged or marked. Devising the system of tags and codes is a critical step. Counsel should give careful consideration to how they may want to sort the data as the investigation progresses and devise codes that will make that work efficient. On the other hand, counsel should take care not to include so many codes that the review will be unduly slowed or overly confusing to reviewers.

If the need to produce documents to outside parties is likely, responsive documents should be reviewed to see if they are privileged and, if so, which privilege would apply. Disclosure of privileged material to a third party, even the government, can in some instances constitute a waiver of privilege, although steps can be taken to limit the scope of such a waiver.

See Chapter 36 on privilege

In the context of an investigation, gathering material is a dynamic process. Discovery of documents will often require follow-up interviews, and information gleaned in interviews may reveal the need for additional search terms or custodians. Documents retrieved from one custodian may reveal that a previously unknown custodian may have responsive material. The document preservation notice and review protocol should be updated as needed throughout the course of the investigation as this information comes to light.

6.7 Documents located abroad

When documents are located in jurisdictions outside the United States, the first step is to look at the relevant country's data privacy and bank secrecy laws (or whether blocking statutes or state secrecy laws are implicated), many of which may seem counter-intuitive to US practitioners.[19] In the European Union, for instance, employees' personal data can only be collected and processed under certain conditions, and law firms and their clients must protect this data from misuse and respect certain rights of the individual data owners.[20] These requirements and the penalties for non-compliance have been heightened by the recent implementation of the General Data Protection Regulation (GDPR), which superseded the Data Protection Directive governing data privacy and applies directly throughout the European Economic Area. Some countries also have procedural requirements (e.g., notification to a works council) that govern the processing, transfer, storage, maintenance and access to documents.[21] Given the heightened scrutiny surrounding personal information, counsel should take care to collect and store only what the investigation requires, and consider whether any special arrangements, such as a cross-border data transfer agreement, would help mitigate collateral risk.

See Chapter 40 on data protection

In the past, corporate counsel has sometimes relied on these foreign laws to avoid producing documents located abroad to US authorities. Recently, DOJ officials have expressed increasing scepticism toward explanations that documents cannot be provided to the DOJ in the United States because of data privacy restrictions, and, by virtue of handling many cases implicating foreign laws, have themselves become knowledgeable about their limitations and exceptions. In the DOJ's view, '[c]orporations are often too quick to claim that they cannot retrieve overseas documents, emails or other evidence regarding individuals due to foreign data privacy laws . . . . A company that tries to hide culpable individuals or

19 In some cases, data privacy regimes can also apply to documents located within the United States if the data resides there in connection with the activities of a non-US entity. This is true, for example, of the European Union General Data Protection Regulation, which has extraterritorial effect in certain circumstances.

20 See the EU General Data Protection Regulation adopted in April 2016, which came into effect on 25 May 2018 and superseded the EU Data Protection Directive (Directive 95/46/EC). Other notable data privacy laws include Hong Kong: Personal Data (Privacy) Ordinance (Cap 486), Japan: the Act on the Protection of Personal Information (Law No. 57 of 2003) and Russia: the Russian Federal Law 'On Personal Data' (No. 152-FZ).

21 See, e.g., articles 91, 96 and 96a of the Austrian Labour Constitution Act (*Arbeitsverfassungsgesetz* – ArbVG).

otherwise available evidence behind inaccurately expansive interpretations of foreign data protection laws places its cooperation credit at great risk.'[22] In 2015, the then head of the Criminal Division at the DOJ, Leslie Caldwell, stated that while 'some foreign data privacy laws may limit or prohibit the disclosure of certain types of data or information', the DOJ nonetheless will challenge what it perceives to be 'unfounded reliance on these laws' and encouraged companies to refrain from 'making broad "knee jerk" claims that large categories of information are protected from disclosure'.[23] The following year, Caldwell reiterated that the DOJ was leveraging its relationships with foreign enforcement partners 'to obtain information when non-cooperative companies make invalid assertions about particular data privacy laws in an effort to shield themselves from [DOJ] investigations'.[24]

This is not to say that companies should disregard or be cavalier with foreign data privacy laws. But counsel should look for solutions to this issue. Where potential strategies exist – even creative ones – for obtaining relevant documents that are located abroad, United States authorities have clearly indicated they expect companies to do so to receive co-operation credit. This will almost always require coordination with skilled counsel in the relevant jurisdiction where the documents are located.

22 Remarks by Principal Deputy Assistant Attorney General for the Criminal Division Marshall L Miller at the Global Investigations Review conference, New York, N.Y., United States, 17 September 2014, available at https://www.justice.gov/opa/speech/remarks-principal-deputy-assistant-attorney-general-criminal-division-marshall-l-miller.

23 Remarks by Assistant Attorney General Leslie R Caldwell at the Compliance Week Conference (19 May 2015), available at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-compliance-week-conference.

24 Remarks by Assistant Attorney General Leslie R Caldwell at the American Bar Association's 30th Annual National Institute on White Collar Crime (4 March 2016), available at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-american-bar-association-s-30th.

7

Witness Interviews in Internal Investigations: The UK Perspective

Caroline Day and Louise Hodges[1]

7.1 Introduction

Witness interviews are a key part of most corporate investigations. While documentary evidence can provide the underlying facts of a case, it is often the accounts given by witnesses that deliver the context and detail of what has happened. They can provide vital background information, shed light on the motivations of those involved and allow for an individual's credibility to be assessed. However, the timing, preparation, record-taking, content and use of the interviews need careful consideration.

Witness interviews can serve a number of purposes in the context of a corporate investigation, including:

- to scope the investigation;
- to understand the facts and issues;
- to understand accountability and defences; and
- to assess the credibility of individuals and their accounts.

Interviews in this context can present particular difficulties because of the myriad employment, criminal, civil and regulatory issues that can arise, and the fact that the interests of the company and the witness are often not aligned. These interviews are typically conducted confidentially and can be premised on a need to maintain legal privilege and the duty of confidence owed between an employer and employee. This can often be at odds with the expectations of some authorities for the company to provide details of the witnesses' accounts. There is often a tension between a company's right to conduct its own enquiries into allegations

1 Caroline Day and Louise Hodges are partners at Kingsley Napley LLP. The authors would like to thank Will Hayes, an associate at Kingsley Napley LLP, for assistance with this chapter.

of wrongdoing, including interviewing its employees, and the suggestion by the authorities that its enquiries could (depending on how they are conducted) be detrimental to a criminal or regulatory investigation. In addition, the position surrounding legal privilege in the context of witness interviews has become more complex over the past few years following a number of court judgments.

This chapter explores these issues, considers the practices that can be adopted when conducting interviews and highlights some of the benefits and risks of these different approaches. It considers the preparation and formalities that may be required for witness interviews in the United Kingdom, and identifies particular complexities that can arise in global investigations when multiple jurisdictions are involved.

Types of interviews 7.2

Broadly speaking, witness interviews in corporate investigations can be split into two categories: preliminary or scoping interviews, and substantive interviews. Generally, they should be distinguished from any employment or disciplinary interviews.

Preliminary or scoping interviews may be appropriate at the outset of an investigation to seek background information, identify further sources of evidence, obtain a quick understanding and provide context to an allegation. These interviews will generally take place at the start of the investigation and, depending on the specific circumstances, may take place before any firm view has been reached on the terms of reference or extent of material that will be reviewed. They are more likely to be conducted with employees who may have knowledge of matters under investigation but are not at direct risk of any criticism. It may also be necessary to undertake interviews with whistleblowers at this stage.

See Chapter 19 on whistleblowers

Substantive interviews will generally take place after most, if not all, the relevant material has been reviewed. The purpose is to obtain a detailed understanding of what went on, to provide explanations of key documents in the case and, if necessary, to test the account given. These interviews will often be used to inform an understanding of any individual and corporate liability and any defences. The timing is important and can depend on a number of factors, including the available evidence, whether the authorities are already involved and whether civil and criminal proceedings are contemplated.

Deciding whether authorities should be consulted 7.3

The decision about whether to consult the authorities in advance of a witness interview is not dictated by statute; no statutory framework explicitly requires it and in general terms a company may manage its internal affairs and make enquiries as it sees fit. Therefore, this decision often rests on whether there is an implicit obligation on the company to notify the authorities under its regulatory reporting regime, or whether it is in the interests of the company to co-operate with the authorities by notifying them of any forthcoming interviews.

Regulated firms may be obliged to report a violation or allegation of wrongdoing. For example, the Solicitors Regulatory Authority's code of conduct

requires a law firm to report any allegation of serious misconduct promptly, fully co-operate with its investigation and report any material change about the firm.[2] Accountants may hold similar obligations under the requirements of their regulators. There are reporting requirements under the Listing Rules for those companies admitted to trading on a regulated market,[3] and those in the regulated sector are required to submit a suspicious activity report if they know or suspect (or have reasonable grounds for knowing or suspecting) that another person is engaging in money laundering or terrorist financing.[4] Financial institutions regulated by the UK Financial Conduct Authority (FCA) must under Principle 11 of the FCA's Principles for Businesses act in an open and co-operative manner and disclose anything relating to the firm of which the regulator would reasonably expect notice.

The FCA's expectations under Principle 11 extend to requiring a firm to consider notifying it of a decision to investigate conduct concerns at the earliest opportunity. In November 2015, the Director in Enforcement at the FCA, suggested during a speech[5] that self-reporting is the bare minimum that is required and that a firm should discuss the scope of its investigation with the FCA as early as possible. He identified witness interviews as a key area of risk, suggesting that firms be alive to the possibility that their own investigation could prejudice or hinder a subsequent FCA investigation, and that firms should discuss this with the FCA before taking action. A firm should therefore consider its regulatory obligations when assessing if, and when, to consult its regulator regarding any proposed witness interviews.

During a speech at the 2nd Annual GIR Live London conference,[6] the then-Director in Enforcement at the FCA recognised that there are sometimes good reasons for firms to carry out their own investigations and that the FCA encourages this proactive approach and does not wish to interfere with a firm's legitimate procedures and controls. However, he reiterated that when conducting their own investigations, firms should ensure that they do not take steps that might prejudice or obstruct a subsequent FCA investigation and highlighted the importance of early communication in this regard.

The Serious Fraud Office (SFO) has similarly acknowledged that there are good and proper reasons for a company to carry out its own investigation[7] but has also referred to the potential dangers of an internal investigation 'churning up the crime scene', which could include the taking of first statements from witnesses

2 Solicitors Regulatory Authority (SRA) Code of Conduct, Chapter 10.

3 Also see Prospectus Rules and Disclosure and Transparency Rules.

4 Part 7 Proceeds of Crime Act 2002 and Part 3 Terrorism Act 2000.

5 Speech by Jamie Symington, then Director in Enforcement (Wholesale, Unauthorised Business and Intelligence), FCA, at the Pinsent Masons Regulatory Conference 2015, 5 November 2015.

6 Speech by Jamie Symington, then Director in Enforcement (Wholesale, Unauthorised Business and Intelligence), FCA at the 2nd Annual GIR Live, London, 28 April 2016.

7 Speech by Alun Milford, then SFO General Counsel, at the 14th Annual Corporate Accountability Conference, Congress Centre, London, 9 June 2016 (as reported by GIR on 10 June 2016).

in a way that influences their testimony.[8] In August 2019, the SFO published its Corporate Co-operation Guidance, which sets out how the SFO assesses co-operation from business entities and its potential benefits.[9] Within that there is an expectation by the SFO that companies would consult in a timely way before interviewing witnesses.

Camilla de Silva, Joint Head of Bribery and Corruption at the SFO, commented in a speech in 2018 that, in the context of the company handling the evidence: 'We need to understand the methodology, what's been captured and from where, the use of search terms and be provided with the metadata. [We a]ppreciate it's likely to be dynamic and not a complete set when you speak to us, so update us as you go along.' On contacting the SFO and the timing of this, she said: 'We will not be offering DPAs in cases of a late conversion to the joys of co-operating; DPAs are a reward for openness – the sooner you come in, self-report and the more you are open with us, the more you have to be rewarded for.' On consulting with the SFO, she said: 'We expect to discuss the scope of the investigation, to be notified of conduct which you uncover and what you ought to bring to our attention even if we don't ask, the sequencing of interviews and media contact.'[10]

Where the authorities are not yet aware of the allegations under review, it is likely that preliminary enquiries will be necessary before the company is in a position to reach a view as to whether to self-report. Where this includes witness interviews, it may be inappropriate for the authorities to be consulted in advance. This can create a tension between the authorities' expectations to be notified as well as the need for the company to bear in mind the risks of prejudicing a future investigation.

See Chapter 3 on self-reporting to authorities

Where an investigating authority is already involved, it is prudent for the company to consult or inform it prior to undertaking interviews. Increasingly the SFO and the FCA have sought to impose restrictions on the conduct of interviews in corporate investigations or to prevent them from taking place. While a company cannot be prevented from undertaking its own interviews, there is risk of criticism if it proceeds without the consent of the authority, particularly where it could be suggested that it has prejudiced an investigation. In particular, there may be circumstances where an investigating authority requests that the company refrain from conducting witness interviews during its investigation. The recent judgment handed down by Mr Justice Williams[11] in the DPA reached between SFO and Serco Geografix Ltd confirmed that: 'The SFO requested that Serco Group PLC and its constituent parts should not engage in any internal inquiry by way of interviewing witnesses during the criminal investigation. There was and continues

8 Speech by David Green QC, then Director of the SFO, at the GIR Roundtable: corporate internal investigations, 27 July 2015.

9 SFO Operational Handbook, Corporate Co-operation Guidance, https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

10 Speech by Camilla de Silva, SFO Joint Head of Bribery and Corruption, at the ABC Minds Financial Services conference, 15 March 2018.

11 *SFO v. Serco Geografix Limited*, Deferred Prosecution Agreement, (Case No. U20190413) [2019] 7 WLUK 45.

to be full compliance with that request. Rather, Serco Group PLC instructed an independent law firm to conduct a full document review and to provide the SFO with a detailed report of its findings.'[12]

7.4 Providing details of the interviews to the authorities

The introduction to the SFO's Corporate Co-operation Guidance sets out its expectations when assessing a company's level of co-operation:

> *Co-operation means providing assistance to the SFO that goes above and beyond what the law requires. It includes: identifying suspected wrongdoing and criminal conduct together with the people responsible, regardless of their seniority or position in the organisation; reporting this to the SFO within a reasonable time of the suspicions coming to light; and preserving available evidence and providing it promptly in an evidentially sound format.*[13]

In a section on 'Preserving and Providing Materials', in relation to a corporate dealing with individuals, the SFO's Corporate Co-operation Guidance lists the following indicators of good practice:

> *i. To avoid prejudice to the investigation, consult in a timely way with the SFO before interviewing potential witnesses or suspects, taking personnel/HR actions or taking other overt steps.*
> *ii. Identify potential witnesses including third parties.*
> *iii. Refrain from tainting a potential witness's recollection, for example, by sharing or inviting comment on another person's account or showing the witness documents that they have not previously seen.*
> *iv. Make employees and (where possible) agents available for SFO interviews, including arranging for them to return to the UK if necessary.*
> *v. Provide the last-known contact details of ex-employees, agents and consultants if requested.*[14]

When it comes to witness interviews, authorities often expect details of the interviews to be provided. It is therefore crucial to consider the purpose of the interview, its intended audience, record-keeping and, if appropriate, how this information is to be shared.

The SFO's Corporate Co-operation Guidance provides that: 'Organisations seeking credit for co-operation by providing witness accounts should additionally

12 *SFO v. Serco Geografix Limited*, Deferred Prosecution Agreement,(Case No. U20190413) [2019] 7 WLUK 45 at para. 24.

13 SFO Operational Handbook, Corporate Co-operation Guidance at p. 1, https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

14 SFO Operational Handbook, Corporate Co-operation Guidance at p. 4, https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

provide any recording, notes and/or transcripts of the interview and identify a witness competent to speak to the contents of each interview.'[15]

There is no statutory duty on a company to co-operate with the authorities with respect to its witness interviews. Instead there is published guidance in the form of codes of practice, speeches and guidelines. This varies between authorities, but for the most part there is an expectation that details of witness accounts should be provided. As the SFO Director, Lisa Osofsky, commented in a recent speech: 'Co-operation is about making the path to admissible evidence easier. This is not rocket science. It is documents. It is financial records. It is witnesses.'[16]

This issue is considered in the Code of Practice on Deferred Prosecution Agreements (the Code)[17] jointly issued by the SFO and the Crown Prosecution Service. The Code states at 2.8.2(i) that co-operation with the authorities will include identifying relevant witnesses, disclosing their accounts and the documents shown to them and, 'where practicable', making witnesses available for interview when requested. The SFO has made clear its expectation that for a deferred prosecution agreement (DPA) to be considered, co-operation must be forthcoming. In the early months of her tenure Lisa Osofsky recalled that: 'I am often asked what prosecutors mean by full cooperation. At its simplest, it's not so hard: Tell me something I don't know. Help the prosecutor find the truth. Don't obstruct, or mislead, or delay. Don't hold things back.'[18]

In 2016, one of the SFO's Joint Heads of Bribery and Corruption at the time commented at a conference: 'There really is a pronounced difference now in the way companies are routinely approaching us – "we think we've got a problem and we're willing to work with you to find out, and if necessary resolve it", not "there's nothing to see here, good luck finding it."'[19] The former Director of the SFO noted in a speech in 2017 that a DPA would not be available to companies under investigation unless they offer 'genuine and demonstrable co-operation'.[20] During a speech in 2018, Camilla de Silva commented: 'To be clear, the co-operation we want is with our investigation into the suspected offence, not the company. This means that, at the end of the process, the company will have helped us move that investigation forward and, in so doing, made it easier for us to investigate and, if appropriate, prosecute other suspects.'[21] More recently, Lisa Osofsky confirmed the SFO's approach in a speech where she stated that companies needed to take

15 SFO Operational Handbook, Corporate Co-operation Guidance, at p. 5, https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

16 Speech by Lisa Osofsky, SFO Director, at the Royal United Services Institute, 3 April 2019.

17 SFO/CPS Deferred Prosecution Agreements Code of Practice, Crime and Courts Act 2013.

18 Speech by Lisa Osofsky, SFO Director, at the 35th International Conference on the Foreign Corrupt Practices Act in Washington, DC, 28 November 2018.

19 Speech by Ben Morgan, then Joint Head of Bribery and Corruption, SFO, at GIR Live New York, 15 September 2016.

20 Speech by David Green QC, then Director of the SFO, at the International Bar Association's anti-corruption conference, Paris, 13 June 2017 (as reported by GIR on 13 June 2017).

21 Speech by Camilla de Silva, SFO Joint Head of Bribery and Corruption, at the ABC Minds Financial Services conference, 15 March 2018.

certain steps for their efforts to count as co-operation: 'First, in carrying out their own investigation, we need to see the ultimate objective of cooperating with law enforcement by preserving vital evidence such as first-hand accounts and witness testimony.'[22]

While the SFO has clearly set out its expectations to be told what witnesses have to say in interviews with particular emphasis on 'first accounts',[23] what is less clear is how the detail of the accounts should be imparted and the level of detail that is required. The SFO has been inconsistent in its approach. In the case of *SFO v. ICBC SB*,[24] it was sufficient for oral reports of first-account witness evidence to be provided by the bank to the SFO to enable full co-operation to be established.[25] Alun Milford, former general counsel at the SFO, noted the bank's commitment to supply all relevant non-privileged material and provision of summaries of witness first accounts as an example of its co-operation.[26]

Summaries of witness interviews were similarly supplied by Rolls-Royce in the context of its DPA reached in January 2017.[27] In his judgment, Sir Brian Leveson, then President of the Queen's Bench Division, noted that the company had demonstrated 'extraordinary cooperation', referring to the disclosure of interview memoranda (on a limited waiver basis) as an example of this.[28] The judgment also made reference to the company 'co-operating with the SFO's requests in respect of the conduct of the internal investigation, to include the timing of and recording of interviews and reporting findings on a rolling basis'.[29] This was referenced further in a speech in 2016 by the then Joint Head of Bribery and Corruption: '[T]hey made available to us written accounts of interviews that took place during the evidence gathering exercise, enabling us to understand both what had happened and the strength of the various accounts given about that.'[30] While the SFO acknowledged its acceptance of summary witness accounts instead of transcripts in the DPAs for Standard Bank and Rolls-Royce, at a conference in April 2017, the former SFO General Counsel refuted suggestions that it would be

22 Speech by Lisa Osofsky, SFO Director, at the Royal United Services Institute, 3 April 2019.

23 Speech by Alun Milford, then SFO General Counsel, to an audience of compliance professionals at the European Compliance and Ethics Institute, Prague, 29 March 2016.

24 *Serious Fraud Office v. Standard Bank Plc* (Now known as ICBC Standard Bank plc): Deferred Prosecution Agreement (Case No. U20150854).

25 Speech by Ben Morgan, then Joint Head of Bribery and Corruption, SFO, at the Managing Risk and Mitigating Litigation Conference 2015, 1 December 2015.

26 Speech by Alun Milford, then SFO General Counsel, at the Handelsbatt Conference 2016, 14 September 2016.

27 *SFO v. Rolls-Royce Plc*, Deferred Prosecution Agreement (Case No. U20170036) [2017] Lloyd's Rep FC 249.

28 *SFO v. Rolls-Royce Plc*, Deferred Prosecution Agreement (Case No. U20170036) [2017] Lloyd's Rep FC 249 at para. 121.

29 *SFO v. Rolls-Royce Plc*, Deferred Prosecution Agreement (Case No. U20170036) [2017] Lloyd's Rep FC 249 at para. 121.

30 Speech by Ben Morgan, then Joint Head of Bribery and Corruption, SFO, at a seminar for General Counsel and Compliance Counsel from corporates and financial institutions, at Norton Rose Fulbright, 8 March 2017.

standard practice in all cases[31] and similarly commented in November 2017 that it is not the case that summaries will always be sufficient.[32]

In the case of *SFO v. XYZ Ltd*,[33] oral summaries were provided without the company's badge of 'genuine co-operation' being compromised. However, the SFO's decision to accept oral proffers in this case has more recently been subject to judicial scrutiny. In *R (on the application of AL) v. SFO*,[34] a judicial review was brought against the SFO for failing to pursue XYZ Ltd for non-compliance with its DPA. The terms of the DPA required the company to disclose to the SFO all information and material in its possession that is 'not protected by a valid claim of legal professional privilege or any other applicable legal protection'. Having accepted oral summaries, and following a number of attempts to pursue the full set of notes, the SFO decided to cease pursuing the full set of notes. The SFO's position in defending the judicial review was that there was no need to obtain the interview notes because XYZ's claims of privilege were 'not obviously wrong', and that it had exercised legitimate prosecutorial discretion in accepting the summaries. Although the application was quashed on the grounds that alternative remedies in the Crown Court were available, and therefore judicial review was not the appropriate action to take, the SFO was criticised in the judgment for not pursuing the disclosure. Mr Justice Green described the provision of summaries as an alternative as 'highly artificial' and questioned the SFO's decision not to take a more robust stance. The SFO was similarly criticised for its failure to challenge the assertion of privilege and require the notes in circumstances where it believed the material not to be privileged. The observations made by the High Court will no doubt encourage the SFO to take a robust approach to the disclosure of interview notes and claims to privilege; while the SFO's approach has not always been consistent, it is unlikely that the SFO would accept oral summaries for key witnesses in future.

Despite the inconsistency in how details of accounts have been disclosed to the SFO, in recent years the SFO has been clear that in order to be considered for a DPA, co-operation is required. Its former General Counsel said in a speech in 2017, '[w]e have been clear and consistent that only co-operative companies will ever be offered the opportunity of entering into a DPA with us.'[35] In *(SFO) R v. Sweett Group PLC* (unreported), Sweett Group's refusal to hand over details of the witness interviews undertaken during its internal investigation was deemed unco-operative by the SFO. The level and extent of co-operation with the SFO will ultimately be determined case by case.

31 Speech by Alun Milford, then SFO General Counsel, at GIR London Live, 27 April 2017 (reported by GIR on 27 April 2017).

32 Speech by Alun Milford, then SFO General Counsel, at the Cambridge Symposium on Economic Crime 2017, Jesus College, Cambridge, 4 September 2017.

33 *SFO v. XYZ Limited*, Deferred Prosecution Agreement (Case No. U20150856).

34 *R (on the application of AL) v. Serious Fraud Office* [2018] EWHC 85.

35 Speech by Alun Milford, then SFO General Counsel, at the Cambridge Symposium on Economic Crime 2017, Jesus College, Cambridge, 4 September 2017.

The FCA similarly expects regulated firms to provide notification of any significant matters that occur in the context of an internal investigation, in accordance with its Principle 11 obligation. While this does not explicitly apply to witness interviews, the FCA Enforcement Guide makes clear that if the FCA is ultimately asked to rely on submissions or an investigation report in the context of its own decision-making powers, it would ordinarily expect the firm to provide the underlying material, which could include notes of witness interviews, in addition to the report itself.[36] While the level of information will undoubtedly differ from case to case, the FCA has indicated that an oral report may not be sufficient and that information should be shared in a transparent manner, with a proper record.[37] Furthermore, if an individual performing a controlled function or a member of senior management is suspended, a firm must submit a Form C explaining the reasons for suspension.[38]

The guidance surrounding co-operation with the authorities and what is expected is evolving. In cases where the company or its employees are at risk of further investigation, prosecution or civil action, the company will want to consider the benefits that early co-operation may bring. However, whether it is in the interests of the company to co-operate will depend on the facts of each case.

7.5 Identifying witnesses and the order of interviews

Where interviews are to be conducted, the company or its representatives, or both, should seek to interview all company personnel who were involved in the facts under investigation, including those who should have been involved by virtue of their position. Reporting lines of those involved should also be considered. The witness list may expand as more information becomes known, and therefore should be reviewed regularly.

Employees generally have a duty to co-operate and are likely to owe a duty of candour towards their employer, and a failure to comply could result in disciplinary action.

See Chapter 19 on whistleblowers

Where there is a whistleblower, it may be preferable to interview him or her at the start of the process. The structure of an investigation is very fact-specific, but, broadly, the order of other interviews should be based on the level of risk that the witness poses to the business, beginning with those who present the least risk to the company. For the most part this is likely to follow levels of seniority, starting with lower-level employees and leaving senior management until later. Timing considerations sometimes mean witness interviews need to be taken out of the normal order. For instance, it is generally advisable to ensure that any employees who may be about to leave the company (either permanently or for temporary absence such as maternity leave) are interviewed beforehand and while they still owe a duty to the company to co-operate. In circumstances where there are a

36 FCA Enforcement Guide, para. 3.26.

37 Speech by Jamie Symington, then Director in Enforcement (Wholesale, Unauthorised Business and Intelligence), FCA, at the Pinsent Masons Regulatory Conference 2015, 5 November 2015.

38 SUP 10.13 Changes to an approved person's details.

number of individuals to be interviewed, consideration should be given to the creation of a 'leavers list' to ensure that potential witnesses who resign from the company are flagged to those undertaking the witness interviews.

See Section 7.6

The benefit of this approach is that the company may be better positioned to obtain an overall sense of the extent of the issues before focusing on particular areas of risk. Lower-level employees are generally more likely to communicate openly, although it is important that sensitive or confidential information is not referred to unless strictly necessary as there is risk that information may be shared.

While it may be appropriate to conduct early interviews with senior employees to obtain initial accounts (particularly where there is likely to be more than one opportunity to interview), generally members of senior management should be interviewed when the investigation is further advanced. Typically, senior employees are more likely to pose a greater risk from the perspective of corporate liability and therefore it is important that any potential risks are identified beforehand. Under the principle of identification, in the United Kingdom a company can be criminally responsible for the actions of those employees that represent the 'directing mind and will' of that company,[39] generally restricted to board directors, the managing director and other senior officers who carry out management functions on the company's behalf.[40] The principle of identification is explored in more detail in Chapter 1.

This can cause difficulties when interviewing board members and senior management who may be the 'client' for the purposes of the investigation but who may need to be interviewed in the context of their own involvement. For the most part this can be avoided by identifying the 'client' at the outset of the case as made up of a group of senior employees or board members with no involvement in matters under investigation. However, depending on the size of the company and the nature of the case, this is sometimes unavoidable and therefore the basis on which the interview is being conducted must be made clear to the witness.

See Chapter 5 on beginning an internal investigation

There are a number of statutory exceptions to the principle of identification, and the government has been examining the case for reform of the law on corporate liability for economic crime;[41] at the time of writing, however, the Ministry of Justice had yet to publish its response to the Call for Evidence.[42] Under section 7 of the Bribery Act 2010, a corporate can be criminally liable for failing to prevent the acts of its employees or agents unless it can show that it had adequate procedures in place to prevent bribery from taking place. Two corporate offences of facilitating tax evasion under the Criminal Finances Act 2017[43] also adopt a failure-to-prevent model, with criminal liability attaching for the acts of persons acting on the company's behalf unless the corporate can show it had reasonable

39 *Lennards Carrying Co and Asiatic Petroleum* [1915] AC 705, *Bolton Engineering Co v. Graham* [1957] 1 QB 159 (*per* Denning LJ) and *R v. Andrews Weatherfoil* 56 Cr App R 31 CA.

40 *Tesco Supermarkets Ltd v. Nattrass* [1972] AC 153.

41 Call for evidence: Corporate and Economic Crime – 13 January 2017 to 31 March 2017.

42 HM Government, National Economic Crime Plan 2019-22, July 2019.

43 Sections 45 and 46, Criminal Finances Act 2017.

prevention procedures in place. Similarly a corporate can be guilty of corporate manslaughter if the management or organisation of its activities causes a person's death, and amounts to a gross breach of a duty of care owed by the organisation to the deceased.[44] When the issues under investigation fall within the statutory exceptions, it can be difficult to identify the appropriate individual to interview on behalf of the company. Again, the purpose of the interview and the basis on which it is being conducted needs to be made clear from the outset.

Senior employees are also more likely to owe fiduciary duties to the company and potentially be liable for breaches of those duties and become defendants in civil proceedings by the company. As a result, these interviews should generally take place when the company is in a better position to identify the extent of any breaches.

See Chapter 5 on beginning an internal investigation

Relevant information could also be sourced through interviews with third parties including former employees, customers and contractors. The obvious benefit is that these witnesses may be more forthcoming where there is no risk of disciplinary proceedings. However, third parties cannot generally be required to attend an interview, and unless there is a contractual obligation requiring their attendance, they could refuse to attend. Even in circumstances where a contractual obligation exists this could be difficult to enforce, as could a confidentiality clause. The interview process itself is likely to notify the third party of the investigation and the subject matter under review and depending on the nature of the relationship, it may not be appropriate to interview him or her at that time, particularly when the decision on self-reporting is outstanding. The timing of these interviews would depend on the facts of each case.

7.6 When to interview

The timing of interviews can be influenced by a number of factors, including the stage of the investigation and whether or not any record of interview would be covered by legal privilege. Scoping interviews usually take place at the outset of an investigation, most likely with a few individuals who have a general knowledge of the subject matter under investigation.

See Section 7.11 and Chapter 35 on privilege

Substantive interviews are likely to be most effective once the bulk of any document review has taken place. This will allow for any key documents to be identified and put to the witness, and for questions to focus on the areas of risk. Furthermore it is best to plan for only one interview; while there may be circumstances where a second or third interview is appropriate, it is by no means guaranteed that the witness would agree.

Timing of the interviews can pose particular difficulties when there are competing considerations. For example, it may be necessary to delay when the company has a claim for injunctive relief against individuals, to avoid assets being dissipated in advance of a freezing order being granted. However, it could be that there is only a limited amount of time to interview an employee who is leaving

44 Section 1, Corporate Manslaughter and Corporate Homicide Act 2007.

the company or the company may need to speak to an individual at short notice to assist in an assessment of whether to self-report. Clearly such factors need to be prioritised.

It is important to allow for a degree of flexibility as certain factors outside the company's control can dictate when an interview should take place. Where the corporate investigation is likely to remain an internal review, there is little risk to the company conducting interviews to a timetable that suits it, although the company will wish to consider whether legal privilege would apply. Where there is suspicion of a criminal or regulatory violation and a formal investigation has commenced, there are a number of risks associated with conducting interviews in parallel with these investigations.

See Section 7.11 and Chapter 35 on privilege

As a general point, any interviews with individuals at risk of criminal exposure should be postponed until all evidence has been secured, to minimise the risk of evidence being destroyed. This is particularly important where a criminal or regulatory investigation is likely. Similar concerns apply where the individuals are potential defendants to civil proceedings by the company.

Both the SFO and the FCA place significant emphasis on the first accounts of witnesses, and take the view that they can help inform an understanding of what went on and allow for the accuracy or integrity of a witness to be tested.[45] However, depending on the facts of the case, this view can often be misplaced; the first account given by a witness is not necessarily always the best one, particularly in complex investigations that span a number of years and where there is extensive underlying material. The quality of a witness's evidence can often be improved having been given the opportunity to review the evidence and recall the context. Nonetheless, the SFO and FCA have increasingly sought to place restrictions on interviews of key suspects in corporate investigations and may seek to prevent them altogether.

In such circumstances it may be prudent for a company to seek to agree an approach with the authorities prior to conducting any interviews.

The authorities are also increasingly sensitive to the risks of witness contamination, and a company whose conduct of witness interviews has caused prejudice to a criminal or regulatory investigation could be subject to serious criticism. At best this could involve comment or views that are unhelpful for the company; at worst this could include allegations of perverting the course of justice. In 2016, the then-Director in Enforcement at the FCA, observed that firms must take care not to take steps that might prejudice an FCA investigation and suggested that in certain circumstances it may prefer that a firm does not commission its own investigation, for example, in criminal investigations where alerting the suspects could have adverse consequences.[46] Mark Steward, Director of Enforcement and Oversight at the FCA has commented on the importance of an 'independent public body

45 Speech by Alun Milford, then General Counsel, SFO, to an audience of compliance professionals at the European Compliance and Ethics Institute, Prague, 29 March 2016.

46 Speech by Jamie Symington, then Director in Enforcement (Wholesale, Unauthorised Business and Intelligence), FCA at the 2nd Annual GIR Live London, 28 April 2016.

investigation' being able to conduct itself without 'the crime scene being trampled over'.[47] The SFO has similarly made clear that corporate investigations that 'trample over the crime scene' are unhelpful and that integrity of evidence, especially regarding witness accounts, should be respected,[48] and has noted that internal investigations may result in first statements of witnesses being taken, delivered or recorded in a form which may be less than full and accurate, as opposed to recording the account by way of a transcript.[49] Camilla de Silva, during a speech in 2018, commented: 'The data needs to be identified, collected, preserved and analysed in a way that does not tip off potential suspects into deleting data and protects its integrity and continuity.'[50]

Witness interviews should always be conducted in a manner that minimises the risk of contamination or prejudice.

When a criminal or regulatory investigation is anticipated or already under way, a company may wish to consider engaging with the authorities at an early stage to avoid any criticism that might follow. However, engaging with the authorities may not necessarily be appropriate in every case and runs the risk of loss of control. Each case will need to be assessed on its specific facts and surrounding circumstances.

7.7 Planning for an interview

Interviews in the context of a corporate investigation can be conducted by various people: internal or external lawyers, accountants, forensic experts, specialist investigators, HR or compliance officers, and others. Careful thought should be given to who is best placed to undertake them.

As a general rule, where a company is engaged in a corporate investigation into allegations of criminal or regulatory misconduct, it is preferable to have lawyers (internal, external or both) present at interviews to take notes and identify the key risk areas, to enable confidentiality, and for any claim to privilege to be strengthened. Generally it is preferable for the same person or persons to conduct the interviews of those witnesses who provide similar types of information. This will allow for consistency of approach and for the credibility of witnesses to be more readily assessed. It is also preferable to have two interviewers present to allow for one to take notes while the other asks questions.

Where external lawyers have been instructed, they should generally conduct the interviews. External lawyers often bring (and importantly are seen to bring) expertise, objectivity and independence, which can be very important when

47 Speech by Mark Steward, Director of Enforcement and Oversight at the FCA, at the 14th Annual Corporate Accountability Conference, Congress Centre, London, 9 June 2016 (as reported by GIR on 10 June 2016).

48 Speech by Ben Morgan, then Joint Head of Bribery and Corruption at the SFO, at the Global Anti-Corruption and Compliance in Mining Conference 2015 on 20 May 2015.

49 Speech by David Green QC, then Director of the SFO, at the GIR Roundtable, 27 July 2015.

50 Speech by Camilla de Silva, SFO Joint Head of Bribery and Corruption, at the ABC Minds Financial Services conference, 15 March 2018.

assessing the credibility of the investigation. Although it can bring a degree of formality that can make the experience more daunting for the witness, the use of external lawyers will strengthen a claim to legal privilege.

Where external lawyers have not been instructed, the company may consider resourcing the process internally either by using compliance personnel, internal auditors or HR officers or by using in-house lawyers. Either way, those conducting the interview should not have had any involvement in the allegations under review. While the use of non-lawyers may decrease the levels of concern among employees, in general they may be less skilled in conducting these types of interviews and less familiar with the issues that may arise. In-house lawyers will have a good understanding of the business and legal advice given to the company will generally be privileged in the United Kingdom. However, the protection of legal privilege will not apply to advice given by in-house lawyers in the context of European Commission related investigations,[51] and it may be necessary in those circumstances to engage external lawyers.

See Section 7.11 and Chapter 35 on privilege

Where forensic experts (internal or external) are also engaged it may be prudent to involve them in interviews with key individuals. If so, it is generally advisable for these interviews to be conducted alongside internal or external lawyers to ensure that the contents can be covered by the company's confidentiality and privilege, as appropriate, and to strengthen a claim to this privilege.

Prior to the interview, a core bundle of documents relevant to the particular witness should be prepared. Consideration should be given to whether the witness is given access to documents, either before or during an interview, or as part of staged disclosure, and what documents, if any, should be put to the witness. Referring to documents can be a very useful tool to assist in refreshing a witness's memory and to allow for specific comment. Key documents can be put to provide a better understanding of its content and to give an opportunity for the witness to provide explanation.

In general, copies of confidential or sensitive documents should not be given to witnesses where there is a risk these could be shared or used contrary to the company's interests. In complex matters, providing pre-interview disclosure will enable the witness to prepare; however, where documents are provided to the witness, this should be done on a restricted and confidential basis with the requirement that they are either returned or destroyed at the conclusion of the interview. It is preferable that a witness is not given documents that he or she has not previously seen.

See Chapters 5 and 6 on beginning an internal investigation and Chapter 11 on production of information to authorities

The provision of documents may give rise to data protection issues, particularly in light of the company's obligations under the data protection principles[52] and where multiple jurisdictions are involved.

A detailed interview plan can be useful to ensure that all relevant questions are put to the witness, although the interviewer should not feel restricted by this. In

51 *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v. European Commission*, Case C-550/07 P.

52 Article 5, General Data Protection Regulation.

general, topics should be addressed in a chronological order that develops facts in a logical way.

Regarding the provision of topics in advance of an interview, it is generally helpful to indicate the main areas that may be covered to assist the witness to prepare, particularly where the subject matter is complex. However, giving a list of detailed questions is generally not appropriate, and a witness who has had the opportunity to script his or her answers is less likely to be considered credible. Furthermore, questions are likely to evolve as the interview progresses. There is also a risk that the questions might be shared.

Interviewers should ask questions in a measured and courteous manner with a clear and professional tone. There is little point in adopting an aggressive approach or engaging in lengthy cross-examination; this is unlikely to be effective and could give rise to criticism, or employment or personal injury claims. A skilled interviewer will seek to put the witness at ease before addressing the key topics. Where there are two interviewers, different interviewing styles can often be effective.

7.8 Conducting the interview: formalities and separate counsel

Professional obligations can affect how witness interviews are conducted. Solicitors have a general duty to act in their client's best interests,[53] they must not take unfair advantage of a third party,[54] and they must not take unfair advantage of an opposing party's lack of legal knowledge where they have not instructed a lawyer.[55] These duties do not always align and it is therefore important to balance the competing requirements.

The interviewer should be satisfied that the witness understands the basis on which he or she is being interviewed, the purpose of the interview and the use that could be made of the information provided, because this may impact its admissibility.

In the United States, an *Upjohn* warning is given at the start of the interview, where lawyers are present. This practice is often adopted in many investigations in the United Kingdom, even where there is no involvement of US authorities at that time. The warning sets out that:

- The lawyers represent the company and not the employee/witness.
- Privilege in the interview belongs to the company and not the employee.
- The company might choose to waive its privilege and disclose matters discussed in interview to the authorities.

Upjohn warnings derive from the case of *Upjohn Co v. United States*,[56] where it was held that the privilege that attaches to communications between a company's lawyers and its employees is the company's privilege, and not that of its employees.

53 Principle 4, SRA mandatory principles.

54 Chapter 11, SRA Code of Conduct.

55 Chapter 11, SRA Code of Conduct.

56 *Upjohn Co. v. United States*, 449 U.S. 383 (1981).

While there is no formal requirement for these warnings to be given in the United Kingdom, it is considered best practice to do so.

The witness should be reminded of the confidential nature of the interview and, where appropriate, be told that it is a fact-finding exercise. However, where a company has decided to waive privilege prior to the interview and provide details to the authorities, the *Upjohn* warning may need to be strengthened. The company could consider whether to give a more formal caution, similar to that given by the police when investigating suspects, although this would rarely be required. If necessary, the witness should be told that while not part of a disciplinary process, the information provided could inform a decision on whether to instigate disciplinary action.

The company should consider whether its own legal advisers can advise the witness or whether to allow the witness to have his or her own lawyer in attendance. The company may wish to offer to pay for the independent legal adviser. Clearly a company cannot prevent its employees obtaining legal advice of their own volition and expense; however, it can control who can be present in an internal interview. If an authority investigation is under way, the witness may have contractual rights or rights under an insurance policy (D&O insurance) to fund an independent legal adviser. Former employees may have an indemnification or contractual right as part of their exit package.

Those witnesses who appear to be at little risk of criminal or regulatory exposure are unlikely to need independent counsel to protect them against any risk of self-incrimination, and the provision of an *Upjohn* warning or a similarly worded preamble should suffice. However, a company may nonetheless offer separate legal advice to these witnesses if this would allay their concerns or ensure that appropriate advice is given (including from an employment or civil perspective). Perhaps most importantly, an independent adviser's role will assist preparation and increase the likelihood that the individual will give their best account. Moreover, it is often not easy to predict where risks may be at an early stage.

The provision of separate counsel is particularly important where there may be a conflict of interest between the company and a witness. This can arise where a witness is a whistleblower or at risk of criminal or regulatory investigation or where the company could be implicated in corporate wrongdoing. In these circumstances the interests of the company and the witness may not align and it would be prudent to consider suggesting independent counsel. While this might delay the interview to allow advice to be given, it ensures that the witness has had the opportunity to obtain his or her own legal advice and, depending on the facts, could make the interview more effective. However, the involvement of an independent legal adviser could also result in the witness being less inclined to attend the interview or answer questions, although an employee would then be at risk of disciplinary action for not co-operating.

The decision when to offer independent legal advice can also depend on the account given by the witness, and it may be appropriate to stop interviews if witnesses give an account that indicates that the company has a potential civil claim against them or that they are making potentially criminal admissions.

Ultimately it would be difficult for witnesses to assert that they had not been fully informed where they had been separately represented, or that the interviewer or company had taken an unfair advantage.

7.9 Conducting the interview: whether to caution the witness

Where a witness may be suspected of involvement in a criminal offence, a caution may be considered. A caution is used by police officers and other investigators when conducting interviews of suspects to ensure that any resulting account (or refusal to answer questions) is admissible in criminal proceedings.[57]

Section 67(9) of the Police and Criminal Evidence Act 1984 (PACE) provides that 'persons other than police officers who are charged with the duty of investigating offences' shall have regard to the relevant provisions of the PACE Codes of Practice, and Code C 10.1 of the Codes sets out the requirement to caution.

This duty applies to SFO investigators,[58] but is not restricted to state authorities and can also apply to private store detectives[59] and commercial investigators who are appointed by a company to investigate its employees for the commission of criminal offences.[60] Importantly, however, it does not apply in the context of an internal investigation where the sole purpose is to determine what recommendations should be made to an internal disciplinary panel.[61] It is therefore unlikely to apply in circumstances where an employer investigates allegations that could give rise to disciplinary action and where the sole purpose of the investigation was to inform the company how to respond.

Where criminal offences are being considered, section 67(9) would only apply if the investigator was charged with investigating or charging criminal offences at the time.[62] This scenario would arise in circumstances where the interviews had been delegated to those conducting the investigation and where they were effectively acting on behalf of a criminal authority. It would require the authorities to sanction the taking of a suspect's account with a view to it being used in a criminal trial. In light of the authorities' general reluctance for a company to conduct interviews with suspects, particularly when it involves obtaining first accounts, it is unlikely that this situation would arise, and therefore a caution is unlikely to be required.

7.10 Conducting the interview: record-keeping

A record can be kept of a witness interview in a number of ways. It could be audio-recorded and transcribed. A verbatim record would exist, removing the risk of any challenge to the accuracy of what was said, and the recording would capture the tone and any pause or emphasis, which can often give context and allow

57 Code C, 10.1 PACE Codes of Practice.

58 *R v. Director of the Serious Fraud Office, ex p Saunders* [1988] Crim LR 837.

59 *Bayliss* (1993) 98 Cr App R 235.

60 *Twaites and Brown* (1990) 92 Cr App R 106.

61 *R v. Welcher* [2007] EWCA Crim 480.

62 *R v. Seelig* [1992] 1 WLR 148 and *Joy v. Federation against Copyright Theft* [1993] Crim LR 588.

for an overall assessment. However, it could affect the witness's account by adding an element of formality, potentially having an unsettling effect on the interviewee and making him or her less forthcoming. More importantly, there is significant uncertainty over whether legal privilege would apply to a recording, particularly where the interview has been conducted as a fact-finding exercise. Even where privilege can be properly asserted, it is likely to be challenged by the authorities, and where a transcript exists, the authorities are likely to request a copy.

See Section 7.11 and Chapter 35 on privilege

An alternative approach is for the legal adviser to prepare a note of what the witness has said. Legal privilege is more likely to apply in circumstances where notes contain some form of legal comment, advice and analysis. This may include the lawyer's own impressions and assessment of the interview. Alternatively two sets of notes could be prepared, one containing the factual account and one containing the lawyer's own views. If so, at a minimum, the authorities are likely to seek a copy of the factual account.

The company will need to decide whether to provide the witness with a copy of the note. Where it is likely to rely on the witness's testimony in civil proceedings, it may be helpful to agree a note at an early stage to limit any future challenge to its accuracy. This carries the risk that it may be passed on and any applicable privilege would be lost, and may cause issues if the account is materially disputed.

Where proceedings are anticipated, there are some advantages in preparing a witness statement at an early stage. If the witness decides at a later date not to co-operate or for whatever reason he or she is no longer able to assist, the company may be able to rely on the evidence given, or compel the witness to attend and give evidence having already taken a record of the witness's evidence. However, even if privilege can be maintained, it is likely the authorities would nevertheless seek a copy.

Legal privilege in the context of witness interviews 7.11

Legal privilege in the context of witness interviews raises a number of complex issues and a claim to privilege will be closely scrutinised by the authorities. Over the past few years, the SFO has claimed that it does not want to undermine legal privilege, which is respected as a legal principle and fundamental right. In a speech made in November 2018, Hannah von Dadelszen, then Joint Head of Fraud (now Head of Strategy and Policy) at the SFO, stated: 'We do not, and never have required the waiver of privilege, but if you want to waive privilege that will be viewed as a positive feature. We are very disinterested in privileged material that is the proper legal advice you are receiving from your solicitors.'[63] In June 2018, Camilla de Silva noted: 'Recent cases have highlighted that the SFO will challenge overly ambitious claims to privilege and, in specific circumstances, are obliged to do so.'[64] In March 2016, Alun Milford, then General Counsel of

63 Speech by Hannah von Dadelszen, then Joint Head of Fraud, at the Pinsent Masons Business Crime and Compliance conference, London, 9 November 2018.

64 Speech by Camilla de Silva, Joint Head of Bribery and Corruption, at the 12th International Pharmaceutical and Medical Device Compliance Congress, Vienna, 14 May 2018.

the SFO, made it very clear that the SFO will view 'false' or 'exaggerated' claims to privilege as unco-operative, and notwithstanding his acknowledgement that a claim may be well founded, where a company discloses details of witness accounts it will be viewed as a significant mark of co-operation.[65] Furthermore, a company's decision to structure its investigation so as not to attract privilege will be viewed as significant co-operation. Camilla de Silva noted: 'We are not interested in material that is genuinely privileged. We do however reserve the right to question, probe and where necessary challenge assertions of privilege which are[,] in our view, excessive.'[66]

In a section on 'Witness Accounts and Waiving Privilege', the SFO's Corporate Co-operation Guidance states:

> *In conducting internal investigations, some organisations will have obtained accounts from individuals. . . . Organisations seeking credit for co-operation by providing witness accounts should additionally provide any recording, notes and/or transcripts of the interview and identify a witness competent to speak to the contents of each interview.*[67]

When an organisation elects not to waive privilege, the SFO nonetheless has obligations to prospective individual defendants regarding disclosable materials.

The existence of a valid privilege claim must be properly established. During the investigation, if the organisation claims privilege, it will be expected to provide certification by independent counsel that the material in question is privileged. If privilege is not waived, and a trial proceeds, where appropriate, the SFO will apply for a witness summons under section 2 of the Criminal Procedure (Attendance of Witnesses) Act 1965.

An organisation that does not waive privilege and provides witness accounts does not attain the corresponding factor against prosecution that is found in the DPA Code but will not be penalised by the SFO.

It is clear that if a company chooses not to co-operate with the SFO, it is much more likely that the company would not be offered a DPA, with Camilla de Silva stating that the SFO will only invite a company to enter into a DPA where that company has 'genuinely cooperated with the SFO' and that 'the DPA Code provides that co-operation will include identifying relevant witnesses, disclosing their accounts and the documents shown to them'.[68] This was echoed by Hannah

65 Speech by Alun Milford, then SFO General Counsel, to an audience of compliance professionals at the European Compliance and Ethics Institute, Prague, 29 March 2016.

66 Speech by Camilla de Silva, Joint Head of Bribery and Corruption, at the Herbert Smith Freehills Corporate Crime Conference 2018, 21 June 2018.

67 SFO Operational Handbook, Corporate Co-operation Guidance, at pp. 4-5, https://www.sfo.gov.uk/download/corporate-co-operation-guidance/.

68 Speech by Camilla de Silva, Joint Head of Bribery and Corruption, at the Herbert Smith Freehills Corporate Crime Conference 2018, 21 June 2018.

von Dadelszen in a recent speech, who confirmed: 'We are going to ask a lot of companies who self-report to us.'[69]

However, there is a risk that disclosing information relating to witness interviews could result in a waiver of privilege more generally. Ultimately the information could be shared with authorities in other jurisdictions or be disclosable in civil, or other, proceedings that may not be in the company's best interests. While this risk may in part be mitigated by a limited waiver agreement, this would not necessarily extend to other jurisdictions, and there is a risk that confidentiality may in due course be lost. The Law Society of England and Wales provides guidance to lawyers about their duty to act in the best interests of clients, including maintaining their claim to privilege.

The law surrounding legal privilege and records of interviews is complex and evolving. It has recently been made more complicated by the narrow interpretation of privilege that has been taken in several recent court decisions. These cases are summarised below.

See Chapter 35 on privilege

It was held in *The RBS Rights Issue Litigation*[70] that the interview notes prepared by the bank's legal representatives were not subject to legal advice privilege (it was accepted that litigation privilege did not apply). The court found that, for the purposes of legal advice privilege, the 'client' consists only of those employees authorised to seek and receive legal advice from the lawyer. In relation to interviews with witnesses, it found that privilege does not extend to information provided by employees and ex-employees outside the client group. Furthermore, it was held that in order for the lawyers' working notes of the interviews to attract legal advice privilege, the notes must contain 'some attribute or addition such as to betray or at least give a clue as to the trend of advice being given to the client by its lawyer'.[71] The court held that the bank had failed to demonstrate this.

This judgment was followed by the High Court in *Director of the SFO v. ENRC*.[72] At first instance, Mrs Justice Andrews rejected ENRC's argument that legal advice privilege applied to lawyers' notes of interviews, and found that the question of whether legal advice privilege applied was an evidential one as to whether the notes demonstrated the legal analysis and 'tenor' of the advice.[73] In her judgment, Andrews J referred to examples of the type of evidence required to attract legal advice privilege, to include a qualitative assessment of the evidence or any thoughts about its importance or relevance to the inquiry, or indications of further areas of investigation that the author of the notes considered might be fruitful. It was noted in the judgment that the betrayal of further lines of investigation would not in itself have been sufficient to render the notes privileged.[74]

69 Speech by Hannah von Dadelszen, then Joint Head of Fraud, at the Pinsent Masons Business Crime and Compliance conference, London, 9 November 2018.

70 *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch).

71 *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch) at para. 107.

72 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB); [2017] 1 WLR 4205.

73 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB); [2017] 1 WLR 4205 at para. 97.

74 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB); [2017] 1 WLR 4205 at para. 180.

Applying the case of *Three Rivers (No. 5)*,[75] Andrews J held that legal advice privilege would only apply to communications between the lawyer and those authorised by the company to obtain legal advice on its behalf, and therefore not to employees or former employees more widely.[76]

Andrews J's decision was appealed, and although the Court of Appeal did not need to reach a decision on issues relating to legal advice privilege (because of its decision on litigation privilege, see further below in this section), it nevertheless gave its view (*obiter*) on how it would have decided those issues. The Court would have found that *Three Rivers (No. 5)* had been correctly interpreted by Andrews J (and by courts on other occasions) as having created a general rule that, in a corporate context, only the communications of those employees authorised by the company to seek and receive legal advice on its behalf are capable of attracting legal advice privilege.[77] On this basis, Andrews J was right to conclude that the interview notes were not covered by legal advice privilege. Significantly however, the Court gave a strong indication that it felt *Three Rivers (No. 5)* had been wrongly decided and would have been in favour of departing from that case had it been open to it to do so, although ultimately it felt this is a question that only the Supreme Court can determine.[78]

In addition, it had been argued by ENRC that the interview notes constituted lawyers' working papers and as such were covered by legal advice privilege. While Andrews J had rejected this argument at first instance, the Court of Appeal declined to give a view.[79]

ENRC's claim for litigation privilege was also rejected by Andrews J at first instance, who was not satisfied that, on the facts, litigation was in reasonable contemplation at the pertinent times or that, in any event, the dominant purpose of the documents coming into existence was for use in the conduct of litigation. The High Court held that an SFO investigation was seen as a preliminary step and that a prosecution only becomes a real prospect once evidence is discovered to substantiate the allegation, or where the accusations appear to be true.[80]

The Court of Appeal took a different approach to the availability of litigation privilege to ENRC's interview notes and disagreed with Andrews J's conclusion of the facts, holding that at the time the documents came into existence, ENRC did reasonably contemplate a prosecution by the SFO.[81] While the Court did not necessarily disagree with Andrews J's view that an SFO investigation in itself could not constitute adversarial litigation for the purposes of litigation privilege, it was of the view that:

75 *Three Rivers District Council v. Governor and Company of the Bank of England (No. 5)* [2003] EWCA Civ 474.

76 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB); [2017] 1 WLR 4205 at para. 180.

77 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at paras. 123 and 133.

78 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at para. 130.

79 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at para. 142.

80 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB); [2017] 1 WLR 4205 at paras. 150 to 163.

81 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at para. 93.

> *When the SFO specifically makes clear to the company the prospect of its criminal prosecution (over and above the general principles set out in the [Self-Reporting] Guidelines), and legal advisers are engaged to deal with that situation, as in the present case, there is a clear ground for contending that criminal prosecution is in reasonable contemplation.*[82]

In addition, although the Court did not accept ENRC's alternative argument that once an SFO investigation is in reasonable contemplation so too is a prosecution, it held that in this case the evidence 'pointed clearly towards the contemplation of a prosecution if the self-reporting process did not succeed in averting it'.[83] Furthermore, the Court did not feel that the uncertainty a company inevitably experiences when faced with whistleblower allegations is a bar to litigation privilege.[84] Finally, the Court deemed as erroneous Andrews J's suggestion that litigation privilege cannot apply until a defendant either knows the full details of what is likely to be unearthed or a decision to prosecute has been taken.[85]

As to whether the dominant purpose of the documents coming into existence was for conduct of the litigation, the Court of Appeal was satisfied that this requirement was met in this case and disagreed with Andrews J that ENRC had always intended to show the documents to the SFO, even though it had indicated that it would give full and frank disclosure. It held that just because solicitors prepare a document with the ultimate intention of showing it to the opposing party, that does not automatically deprive the preparatory legal work that they have undertaken of litigation privilege.[86] Of particular importance was the Court's view that documents prepared for the dominant purpose of avoiding or settling litigation are just as much covered by litigation privilege as those prepared for defending it.[87] The Court of Appeal concluded that the interview notes were covered by litigation privilege, as a prosecution by the SFO was in reasonable contemplation at the time they came into existence, and they were created for the dominant purpose of resisting or avoiding it.

ENRC provides very helpful guidance and several principles of wider application to assist corporates who find themselves in similar situations. However, it also highlights the extent to which questions of litigation privilege in the context of internal investigations turn on the facts (as indeed is the case with all questions of privilege).

Three other recent cases also illustrate the importance of the facts of the case when it comes to establishing the status of privilege, and a company should

82 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at para. 96.
83 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at para. 97.
84 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at para. 98.
85 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at para. 100.
86 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at paras. 102 and 112.
87 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006; [2019] 1 WLR 791 at paras. 102, 113 and 118.

consider this throughout the internal investigation so it can better judge whether the notes of a witness interview are likely to be privileged at any stage.

In *Bilta & Ors v. RBS & Anor*,[88] the High Court's Chancery Division was concerned with the status of documents created during an internal investigation carried out by RBS's solicitors, relating to a tax dispute with Her Majesty's Revenue and Customs (HMRC). The documents included transcripts of interviews with employees and ex-employees that had come into existence following HMRC sending RBS a letter claiming there were sufficient grounds to deny it a certain amount of input tax. Bilta and various other claimants subsequently sought disclosure of these documents, which was resisted by RBS on the basis that they were subject to litigation privilege. The Court held that the documents were indeed protected by litigation privilege. As to whether litigation could be said to be reasonably in contemplation at the time the documents came into existence, the sending of HMRC's letter was considered significant and found to have marked a 'watershed moment', and was likened to a letter before claim. While RBS may also have hoped to dissuade HMRC from proceeding, it was found that this was only a subsidiary purpose subsumed into the dominant purpose.

In *R (for and on behalf of the Health and Safety Executive) v. Paul Jukes*,[89] following a fatality at work, solicitors instructed by the employer concerned carried out an investigation. A statement was obtained from the appellant Mr Jukes, a former manager, as part of the internal investigation, after the Health and Safety Executive (HSE) had begun its investigation but before it commenced proceedings. This statement was relied on heavily during the subsequent prosecution of the appellant, and following his conviction he appealed, partly on the basis that the trial judge had been wrong to allow the prosecution to rely on the statement, as it was protected by privilege. The Court of Appeal did not accept this argument and found that at the time the statement was made there was no evidence that anybody within the company knew what the company's and the HSE's investigations would unearth, such that it could be said that prosecution by the HSE was reasonably in contemplation. It was held that the statement was not therefore protected by litigation privilege.

In *Jukes*, the Court of Appeal approved part of the first instance *ENRC* decision. The Court of Appeal in *ENRC* addressed this potential issue but felt that its conclusions were not invalidated by *Jukes*, on the basis that the endorsement of Andrews J's judgment in that case had been *obiter*.

Notes of interviews and the status of privilege were further considered by the High Court in *R (on the application of AL) v. SFO*.[90] A judicial review was brought against the SFO for failing to pursue an anonymised company, XYZ Ltd, for non-compliance with its DPA through not disclosing the full interview notes,

88 *Bilta & Ors v. RBS & Anor* [2017] EWHC 3535 (Ch).

89 *R (for and on behalf of the Health and Safety Executive) v. Paul Jukes*, [2018] EWCA Crim 176.

90 *R (on the application of AL) v. SFO* [2018] EWHC 856 (Admin).

having instead accepted oral proffers.[91] The SFO's position was that there was no need to obtain the interview notes because XYZ's claims of privilege were 'not obviously wrong',[92] and that it had exercised legitimate prosecutorial discretion in accepting the oral proffers. In the judgment, the SFO was criticised for (among other things) its failure to challenge the assertion of privilege and require the notes in circumstances where it believed the material not to be privileged. It was found that, even if the assertion of privilege could be made out (which, in light of recent case law, the court said was not supported), by providing oral summaries the privilege had been waived. The judgment noted the SFO's failure to fully consider whether to require XYZ to waive privilege over the notes, given its contractual duty to co-operate under the DPA,[93] and whether privilege had been waived, even on a limited basis.

At the time of writing and in the absence of any further judicial interpretation, those conducting internal investigations should therefore be conscious that a claim to privilege of records of interviews with those outside the client group could be subject to challenge, notwithstanding the helpful decision of the Court of Appeal in *ENRC*, and whether a claim to privilege will be successful will depend on the facts of each case. Where the records could be said to form part of the lawyer's working papers in the context of advice, a claim to legal advice privilege would be strengthened if the notes contained sufficient legal analysis, assessment as to relevance and the 'tenor' of the legal advice. Legal advice privilege will also attach to material that forms part of the continuum of the lawyer–client communications even where those documents do not expressly seek or convey legal advice.[94] For litigation privilege to apply, however, litigation must be in reasonable contemplation, and the dominant purpose of the interviews must be the conduct of that litigation. This will depend on the facts of the case, but where litigation is in contemplation, this should be documented to assist in defending any challenge to a claim for privilege.

See Chapter 35 on privilege

Factors that may strengthen a claim to privilege over interview notes include where, for example, notes arise from interviews with likely potential defence witnesses in contemplated litigation or where interviews are conducted with a view to assessing the potential risk the witness may pose in likely proceedings.

Those conducting investigations may wish to consider the timing of witness interviews in the context of when the likelihood of litigation (civil or criminal) is clearer, in the absence of which there is a risk that claims to privilege of records of witness interviews will be challenged.

Where privilege can be established, the best position may be to ensure that any notes taken during interviews are done so as to strengthen a claim to privilege

91 *SFO v. XYZ Ltd* (Case No. U20150856). The defendant was subsequently identified in July 2019 as Sarclad Ltd following the acquittals of three Sarclad employees.

92 *R (on the application of AL) v. SFO* [2018] EWHC 856 (Admin) at para. 7.

93 *R (on the application of AL) v. SFO* [2018] EWHC 856 (Admin) at para. 26.

94 *Balabel v. Air India* [1988] 1 Ch 317.

and to leave any decision on whether to waive privilege until the course of the investigation and interests of the authorities are clearer.

7.12 Conducting the interview: employee amnesty and self-incrimination

As a general point, an employer cannot provide amnesty from criminal or regulatory action. Similarly, an agreement cannot prevent disclosures to regulators or inhibit criminal investigations.

While in theory amnesty against internal disciplinary action could be offered, this is very rare. More commonly, discussions take place with a view to the employee leaving under the terms of a settlement agreement, which can include a financial settlement and avoids the employee being dismissed. Such discussions can take place 'without prejudice', or they may take place as 'protected conversations' and therefore should not take place during a witness interview. These discussions, providing they meet the required criteria, cannot be used as evidence in unfair dismissal proceedings,[95] although, unless the without prejudice rule can genuinely apply, they could be used in whistleblowing or discrimination claims.

See Chapter 13 on employee rights

Though in theory it is possible for an employer to agree a certain course of action (for example, to retain an employee and waive the right to bring disciplinary action), this would not be advisable in circumstances where facts are not yet known or understood. If an amnesty is given, the employer would want to ensure that any waiver against disciplinary action related to closely defined and identifiable incidents only.

Employers also need to be wary of consistency. Where two employees have committed misconduct, allowing one employee to remain and dismissing another would support an unfair dismissal claim that the dismissed employee may bring. The employer would need to justify the difference in treatment, which may be easier to do when an employee has left under the terms of a settlement agreement.

An employee may also seek to claim privilege against self-incrimination and refuse to answer questions on that basis, particularly where he or she is advised by independent counsel. While there may be clear advantages to this approach from a criminal or regulatory perspective, this in itself would not provide a defence against dismissal. An employer could reach a decision to dismiss on the basis of the information that it had at that time. Though it cannot compel employees to answer questions, their failure to do so could be deemed to be unco-operative and in breach of the terms and conditions of employment, resulting in further grounds for disciplinary action. A dismissal for gross misconduct can still be fair in circumstances where a decision has been made not to prosecute, or where the employee has been acquitted of criminal charges for the same offence.[96] Acts that could constitute gross misconduct are broader than criminal offences and the

95 Section 111A Employment Rights Act 1996.

96 *Okhiria v. Royal Mail* UKEAT/0054/14/LA.

requirement that gross misconduct be 'fair' is lower than the criminal standard of proof.[97]

In addition to employment considerations, it is always possible for an employer to agree not to pursue civil claims against an employee in return for information being provided. However, as set out above, this should generally not be offered until the full facts have been established.

Considerations when interviewing former employees 7.13

In general, unless there is a contractual commitment to do so, former employees can simply refuse to attend a witness interview. It is important to bear this in mind when negotiating an employee's exit, although in reality (depending on the specific contract terms), once the employee has left there may be little a former employer can do to require attendance, even if it enjoys the benefit of a contractual commitment from the employee to co-operate in any future investigation or proceedings. Former employees regulated by the FCA have a duty under Statements of Principle and Code of Practice for Approved Persons (APER) Principle 4 to co-operate with the regulators.[98] It is unlikely that this provision would require them to assist with an internal investigation, and if asked, they could fairly argue that their duty was to the regulator.

Where a former employee is interviewed there are some protections available in respect of whistleblowing, discrimination or victimisation, should they arise in the conduct of the interview or how he or she is treated afterwards. An employer should be wary of giving assurances of anonymity to a former employee in respect of information given, although this could be given on a need-to-know basis. Anonymity should not be guaranteed where regulatory obligations exist or where it could inhibit any criminal investigation, and assurances that any statement provided would not be disclosed to criminal or regulatory authorities should not be given.

See Chapter 5 on beginning an internal investigation and Chapter 11 on production of information to authorities

Data protection issues may also arise if the account or statement given by a former employee contains personal data. Care also should be taken in global investigations that data protection rules from other relevant jurisdictions are considered.

See Chapter 40 on data protection

97 A dismissal for gross misconduct is 'fair' if the employer believed that the employee was guilty of gross misconduct, if it had reasonable grounds on which to base that belief, and if it had carried out as much investigation as was reasonable in the circumstances of the particular case: *British Home Stores Ltd v. Burchell* [1978] UKEAT 108_78_2007. In a criminal trial the standard of proof required is to prove guilt 'beyond a reasonable doubt'.

98 The Statement of Principle 4 (see APER 2.1A.3 R) is in the following terms: 'An approved person must deal with the FCA, the PRA and other regulators in an open and cooperative way and must disclose appropriately any information of which the FCA or the PRA would reasonably expect notice.'

7.14 Considerations when interviewing employees abroad

Interviewing witnesses abroad can present particular difficulties in global investigations. Statutory employment law is generally of geographical rather than universal jurisdiction and, as a result, statutory employment laws of the jurisdiction where an employee is based will always apply, even if the employment contract is governed by English law. Nonetheless the governing law of the contract should also be considered, as should any rights or protections under that contract.

When planning interviews abroad it is crucial that the law and procedure relevant to those jurisdictions are considered. The employment documents (the staff handbook, for example) should be reviewed to ensure that procedures are followed. It is important to consider whether the employee or employer is covered by any regulatory rules within that jurisdiction (as well as the United Kingdom) to ensure compliance with any parallel reporting obligations.

It would be wise to engage local legal advice on local laws and local culture, which should be factored into the interview strategy. Clearly the interviews should comply with local laws, and in particular those relating to employment, data protection, privacy and privilege. While the English rules of privilege determine whether privilege applies in this jurisdiction, authorities from other jurisdictions may also have an interest, and advice should be sought on how privilege is determined in those jurisdictions.

A witness's procedural rights in the jurisdiction where he or she is based, as well as in the United Kingdom, should also be considered. Compliance with local laws as well as collective consultation and representation rules should be factored in. In addition, the employer should take advice on whether the employee abroad is covered by UK statutory employment rights.

See Chapter 5 on beginning an internal investigations and Chapter 40 on data protection

Issues often arise regarding access to documents, particularly where there are restrictions on the movement of information from one jurisdiction to another.[99] Employees may also have a right to access and correct notes and files identifying them.[100] The applicable directives, regulations or rules should be considered in advance to ensure compliance with data protection laws.

Finally, maintaining confidentiality can be particularly difficult when interviewing witnesses abroad. Where witness interviews span a number of countries, the risk of information being shared or leaked is greater and measures should be put in place to ensure that confidentiality remains.

7.15 Key points

Witness interviews are a key part of most internal investigations and can provide vital information for the investigation. Internal investigation interviews can take the form of either preparatory interviews at the outset of an investigation or

99 The General Data Protection Regulation sets limits on the collection and use of personal data within the EU. The provisions were supplemented by the Data Protection Act 2018 (passed 23 May 2018).

100 Right of access by the data subject, Article 15 of the General Data Protection Regulation.

substantive interviews likely to take place once a review of relevant material has taken place.

There can be a tension between the right of a company to investigate allegations of wrongdoing and undertake witness interviews as part of its review, and the expectations of the authorities to be consulted prior to it doing so. Enforcement agencies may seek to restrict how the interviews are conducted or suggest that they be postponed until the authorities have conducted their own investigation. Witness interviews should be conducted in a manner that minimises the risk of contamination or prejudice.

UK enforcement agencies have stated that a refusal to provide details of the accounts given by witnesses in internal investigations could be construed as unco-operative or a breach of regulatory requirements. The provision of this information and the form in which it would be provided needs to be balanced with the need to ensure confidentiality in an investigation and to maintain legal privilege.

Where a company is investigating allegations of criminal or regulatory misconduct, it is preferable to have lawyers (internal, external, or both) present at interviews to take notes and identify the key risk areas that may arise, and to enable confidentiality and for privilege to be asserted, as appropriate. Where external lawyers have been engaged it is preferable for them to conduct the interviews; they often bring (and, importantly, are seen to bring) expertise, objectivity and independence. Preferably there should be two interviewers to ensure all relevant information is captured.

Interviews can be recorded in a number of ways: by recording and transcribing the interview; by counsel preparing notes of the interview; and with the preparation of a witness statement. UK and overseas enforcement agencies are likely to seek details of the accounts provided, and consideration should be given to ensuring legal privilege is capable of being asserted. How an interview is recorded, the privilege that may attach to that record, and whether or not to provide details of the witness's account will depend on the circumstances of each case.

Legal privilege in the context of witness interviews raises a number of complex issues and a claim to privilege will be closely scrutinised by the authorities. Notes of interviews with witnesses who fall outside the 'client' group may attract litigation privilege if circumstances allow, but the facts of each case must be carefully considered. There is a risk that disclosing information relating to witness interviews could result in a waiver of privilege more generally.

When conducting the interview, lawyers should be satisfied that the witness understands the basis on which he or she is being interviewed, the purpose of the interview, and the use that could be made of the information provided. While there is no formal requirement to do so, it is best practice for the witness to be given an *Upjohn* warning at the outset and to remind the witness of confidentiality. Where a company has decided to waive privilege prior to the interview, the *Upjohn* (or similar) warning may need to be strengthened. It is unlikely that a formal caution, similar to that given by the police when investigating suspects, would be required.

The company should consider whether its own legal advisers can give advice to the witness or whether to offer (and to pay for) separate independent legal advice, particularly where there may be a conflict of interest between the company and the witness and where the witness is at risk of criminal or regulatory investigation, or where the company could be implicated in corporate wrongdoing.

In general, a company cannot provide a witness with amnesty from criminal or regulatory action. Similarly an agreement cannot prevent disclosures to regulators or inhibit criminal investigations. Amnesty against internal disciplinary action is rare and while it is always possible to agree not to pursue civil claims in return for information being provided, this should generally not be offered until the full facts have been established.

Interviewing witnesses abroad can present particular difficulties in global investigations. It is crucial that the law and procedure relevant to those jurisdictions are considered and that any relevant regulatory rules are complied with. It would be wise to engage local counsel to advise on local laws, regulatory rules and culture to ensure compliance. Any applicable directives or regulations surrounding access to documents should also be considered in advance to ensure compliance with data protection laws. Measures should be put in place to seek to ensure confidentiality.

8

Witness Interviews in Internal Investigations: The US Perspective

Anne M Tompkins, Jodi Avergun and J Robert Duncan[1]

Introduction 8.1

The white-collar practitioner's interview of a company employee or officer is often the main event of an internal investigation or review. Significant planning and execution are required, however, well before a lawyer steps into the interview room. Whether a witness interview is part of an internal or regulator-facing investigation, or general proactive review, they must be designed to extract the necessary information. Some witness interviews may be designed to gain a level of understanding about business operations or controls present in an organisation, while others may seek to determine corporate or individual culpability after a whistle is blown or an accusation levelled. In each case, the white-collar practitioner must focus his or her planning and resources on uncovering the most relevant information. This chapter provides practical considerations to prepare for, perform and report on witness interviews in the typical white-collar case.

Preparation for the interview 8.2

A good interview process starts with identifying the individuals with potentially relevant information to the investigation. In some cases, as with a specific whistleblower allegation, identifying the right interviewee may be easy. Larger or less well-defined reviews require more planning with respect to identifying the interviewees. One practical way to start is to obtain organisational charts, which will allow the practitioner to see reporting relationships and the relative rank of employees within the organisation. Speaking to a mixture of both high- and low-ranking employees can assist in collecting a broad base of information. Although attorneys

1 Anne M Tompkins and Jodi Avergun are partners and J Robert Duncan is an associate at Cadwalader, Wickersham & Taft LLP.

often focus on higher-ranking employers, lower-ranking employees are closer to the day-to-day operations of an organisation and can provide needed insight into operations and employee relationships.

Attorneys should be prepared, and even expect, that some employees will not have the knowledge they are seeking or may not have the expected information. Flexibility is important, as interview time is valuable. If chosen carefully, almost all interviewees will have some valuable information, even if the expected information is not available from a particular interviewee. But, when the interviewee lacks the relevant information, careful consideration should be given to cutting a non-productive interview short to avoid unnecessary costs and to leave time for more substantive conversations later.

Once interviewees are chosen, a practitioner should consider the order in which witnesses will be interviewed. Generally, it is best to start with interviewees that may have background information to gain familiarity with the subject of the investigation and general information about both the industry and the particular practices of the company. Background interviews also help define the parameters of more specific and focused interviews of later witnesses. As the interview schedule progresses, more discrete and specific issues can be the focus. If possible, it is best to interview employees in surroundings that are comfortable to them – generally in a conference room at their place of employment. However, certain sensitive interviews may be better conducted at a third-party location, such as a hotel conference room nearby to the interviewee's home or office. It is important that the interviewee feel comfortable to speak freely and honestly, which may dictate a meeting outside the workspace and away from co-workers and supervisors to avoid the perception of corporate control.

Attorneys usually rely on outlines to guide the interview. An outline will annotate the main issues and information sought and provide a checklist to make sure all planned topics are covered in the interview. Key questions or points can be listed to aid in the interview process and flow. Relevant background information, such as key dates or events, or excerpts from key emails should also be included to aid in the event that an interviewee does not recall important details. In addition, an outline will highlight specific documents or exhibits that will be covered with an interviewee to aid in refreshing the witness's memory or elucidating statements made by the witness. The interviewer should, however, remain nimble and be able to veer 'off script' if unexpected information surfaces during the interview. Preparation is key, but not at the expense of gaining valuable information.

Finally, when preparing for interviews in locations outside the United States, planning for the interview should account for local data-privacy laws and blocking statutes and the need for interpreters. Attorneys should understand before conducting interviews abroad any restrictions on recording interviews and leaving the country with notes taken during an interview. Interpreters should be used unless the interviewee is native-language proficient in the language of the interviewer to avoid any misunderstandings. Because it is likely that the interview will deal with complex and technical subject matter, even highly proficient speakers may struggle with some topics.

Upjohn protections 8.3

When a practitioner who represents a corporate client is interviewing an employee, it is important that the attorney ensure that the witness understand the limitations of an attorney's representation and issues surrounding privilege. This is commonly referred to as an *Upjohn*[2] warning, and entails informing the witness that the attorney represents the company, not the witness individually. In addition, the attorney should inform the employee witness that:

- counsel has been hired to gather information for the purposes of providing legal advice to their client – the corporation;
- their fact-gathering is protected by both attorney–client communications and work-product privilege;
- that privilege belongs not to the witness, but to the company, and it is the exclusive decision of the company whether to waive that privilege – which it can do at any time; and
- the witness must keep the interview and what is discussed during it private and confidential.

Following an *Upjohn* warning, attorneys should ensure that the witness understood the warning and document that the *Upjohn* warning was given and understood.

A witness is likely to have questions after being given an *Upjohn* warning – the most common being 'do I need my own attorney?' Attorneys must take care to develop a strategy for responding to such questions. It is not proper for the attorney to provide legal advice to the witness, having just explicitly disclaimed an attorney–client relationship with that individual. If a witness persists in requesting legal advice, an attorney should confer with internal company counsel, who may then offer the employee names of potential attorneys with whom the witness can consult. Telling the witness that they need their own counsel could constitute legal advice, so attorneys should, wherever possible, refrain from doing so.

See Chapter 14 on employee rights

Protecting work-product and attorney–client privilege 8.4

In the United States, there are two main types of privilege that may protect work-product and communications during an internal investigation: attorney–client privilege and work-product privilege. The attorney–client privilege protects communications between an attorney and his or her client to encourage full and frank communication without fear that confidential information will be disclosed to others.[3] Work-product privilege is broader than the attorney–client privilege, but it does not extend to every document generated or reviewed by the attorney.[4] Work-product privilege applies to materials prepared in the anticipation

2 See *Upjohn Co. v. U.S.*, 449 U.S. 383, 385 (1981) (stating the privilege protects communications between the client and the attorney, not the underlying facts).

3 *Swidler Berlin v. United States*, 524 U.S. 399, 403 (1998).

4 *NXIVM Corporation v. O'Hara*, 241 F.R.D. 109, 126-27 (N.D.N.Y. 2007).

of litigation, litigation in process, or the prospect of future litigation, and reflects litigation investigation or analysis.[5]

There are many best practices to protect communications and documents – including notes as discussed more fully below – under both privilege doctrines. First, to establish and document the attorney–client relationship and basis for work-product privilege, the corporation should state in writing that the attorney has been hired to conduct an internal investigation in anticipation of government or civil litigation. Corporations can even include this language in their company policy regarding internal investigations. Secondly, although internal investigations are largely a fact-finding mission that do not necessarily require an attorney, it is important to ensure that there is sufficient attorney oversight and involvement in the investigation. Even though the privilege can extend to conversations with a non-attorney as long as that person acts as an agent of the attorney, it is always safer to consistently involve corporate and external counsel in these conversations. Counsel should routinely document that the investigation is made to render legal advice and that these communications are privileged and confidential. This can be accomplished by both marking documents as 'Privileged and Confidential' and giving witnesses an *Upjohn* warning, informing them of their relationship to counsel and that all communications are confidential.

See Chapter 36 on privilege

Practitioners conducting investigations outside the United States must be aware of different standards for privilege and adjust accordingly. What may be privileged in the United States may be discoverable in other jurisdictions. For example, in the United Kingdom the attorney–client privilege is limited only to discussions of legal advice between an attorney and his or her client – the 'client' may not include lower-level company employees who do not have the authority to seek and receive legal advice on behalf of the company.[6] In addition, the United Kingdom does not extend protection to communications with third parties, even where those third parties, such as accountants, were engaged to assist or enable an attorney to provide legal advice to the client.[7]

8.5 Note-taking and privilege

To ensure that witnesses are comfortable and candid, less formal note-taking should be considered. For example, some attorneys find that typing notes on a laptop during an interview is distracting or intimidating to the witness, so lawyers should be ready to handwrite their notes if this would lead to a better interview outcome. While this may increase witness comfort, it decreases efficiency, as such notes are almost certainly going to have to be typed at a later date. For one or two

5 Fed. R. Civ. P. 26(b)(3); Restatement of the Law, Third, Law Governing Lawyers § 136 – Work Product Immunity.

6 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* (2017) EWHC 1017 (QB) at para. 70.

7 Bankim Thanki QC et al., 'Privilege: The UK Perspective' in *The Practitioner's Guide to Global Investigations*, ¶ 35.3.2.1 (3d ed. 2019).

interviews, this is reasonable, but when interviewing a dozen or more individuals, typing up handwritten notes will be a burdensome task.

Special attention should be paid to how notes are taken for the purpose of discoverability under the work-product privilege doctrine. Under the doctrine, protection attaches to the 'thoughts and impressions' of attorney work-product and these thoughts and mental impressions have often been afforded the strongest protections under the principles of evidence and civil procedure.[8] The decision to take notes as opposed to typing a verbatim transcript carries important implications under these doctrines of which interviewers should be aware before making a decision on their preferred method during an interview. Protecting privilege requires a complicated analysis and varies significantly based on the jurisdiction in which the investigation will occur.

For example, if privilege protection regarding the notes of an interview was challenged, it is less likely – in most jurisdictions – that a court would characterise a verbatim transcript as containing the 'thoughts and impressions' of the attorney. Such a ruling would increase the likelihood of its discoverability.[9] Note-taking including summaries and thoughts, on the other hand, is more likely to contain the thoughts and mental impressions that the attorney has throughout the interview, eliciting work-product protection and making this approach both more helpful to the attorney when reviewing the topics discussed in the interview in addition to reducing the likelihood of discoverability. One approach is to take notes on the same, or slightly modified, document used to create the outline. This approach makes it easier for the note-taker to follow the topics in the interview and notify the interviewer of any missed topics, and increases the likelihood that the note-taker will record thoughts and impressions rather than verbatim conversations.

On the other hand, verbatim transcripts are not necessarily without privilege protection and can certainly be helpful if the investigator knows for certain that they will need to recall exactly what has been said during an interview. Depending on the type of interview being conducted or the type of business taking place at the firm under investigation, certain interviews may be extremely fact-intensive and require greater precision during the note-taking. For example, if the investigation hinges on the steps and processes employed throughout a complex financial transaction, it may be beneficial to have a full transcript to review the steps and

8 See *Hickman v. Taylor*, 329 U.S. 495 (1947).

9 Courts across the United States are inconsistent on the protection of verbatim transcripts, even when prepared in anticipation of or during litigation. Therefore, the safest course of action when privilege protection is paramount is to prepare notes that reflect the 'thoughts and impressions' of the attorney taking them. Compare *Nam v. U.S. Express, Inc.*, 2012 WL 12840094, at *3 (E.D. Tenn. 15 May 2012) (holding that recordings of non-party witness interviews were not privileged because they were merely recitations of facts and did not contain mental impressions, conclusions, opinions or legal theories of a party's attorney concerning the litigation), with *Hatamian v. Advanced Micro Devices, Inc.*, Case No. 14-cv-00226-YGR (JSC), 2016 U.S. Dist. LEXIS 60551, at *4 (N.D. Cal. 6 May 2016) (preventing discovery of verbatim interview notes as factual work-product).

processes in the future. The need for the protection of privilege versus the need for exactness must be weighed.

Immediately following an interview, and before the commencement of the next interview on the schedule, the interviewer and note-taker should confer about the interview, allowing the note-taker – who is usually the more inexperienced party – to jot down any other notes that may be of use at a later date. Once the interviews have concluded for the day, the note-taker should re-review his or her notes, making appropriate edits to allow for the cleaning up of the work-product at a later date. Finally, when all interviews are complete, the note-taker should prepare a clear and concise document that memorialises the contents of the interview and distils all relevant information for easy recall and access.

There is no correct answer for every investigation, and it is up to the interviewer to use his or her best informed judgement when deciding how to take notes through the interview. In most situations, the specific nature of the investigation and the sensitivity of the information will provide sufficient guidance.

8.6 Interactions with witnesses

One of the first challenges that can take place prior to an interview is the consideration of providing counsel for the witness. Often, companies will provide counsel for the witness so that the witness has an advocate and to avoid creating the false impression that the company's counsel is also charged with representing the witness. If both the company under investigation and the specific employee being interviewed are potentially facing criminal charges, it is generally recommended that the employee retain separate counsel in case the interests of the company and individual diverge. Furthermore, the employer and the employee could consent to enter into a joint defence agreement that will facilitate sharing information, based on their common interests in the investigation and defence.

When considering interactions with witnesses, the interviewer should determine whether there is a company policy on co-operation with investigations. Firms may have policies that require co-operation during internal investigation and knowledge of these policies prior to the interview potentially could serve as a helpful starting point. Certain witnesses may be unaware that these policies even exist – which the interviewing attorney may want to bring to their attention should the need arise.

With respect to conducting the interview itself, it is important to tailor the approach according to the particular witness. If a witness is friendly, and not suspected of wrongdoing, it is important to start by being approachable and personable with the witness to avoid any intimidation and potentially evasive or unhelpful answers. The interviewing attorney should begin the interview in a 'light' and non-demanding fashion to put the witness at ease. If the witness does not feel under pressure from direct and pointed questions, then he or she will be much more likely to share information that pertains to the investigation. If, however, an attorney knows that a witness is likely to be adverse or hostile, a different approach may be necessary. Witnesses may be hostile when they have committed a wrongful act – where information from an investigation or previous interviews

suggests a witness is culpable. When confronting a witness with documents that show guilt or wrongdoing, conducting a cross-examination with leading questions may be more helpful. Regardless of the witness's posture, the interviewer should also allow for questions from the witness. The goal of the interview process is to allow the witness to 'tell their story' while allowing the interviewer to maintain the role of counsellor and listener. Receiving and responding to the witness's questions thoughtfully and respectfully will quickly establish trust and confidence, as opposed to coldness and hostility.

In addition to allowing the witness to 'tell their story', one of the other major objectives of an interview is to ask the witness about other individuals who may have knowledge on the subject of the investigation. When a witness is describing a certain set of events, it is not uncommon for him or her to discuss conversations held with others as these events took place. The interviewer should make sure to follow up on the other individuals that the witness brings up, both in the interview itself and after deciding who else should be contacted as a new witness.

Because each witness will react differently to certain questions, and there is no set formula for conducting an interview, the interviewers should strive to make the interview as open and conversational as possible while ensuring that the information being shared is both relevant and helpful to the investigation as a whole.

Document review and selection 8.7

In the ideal case, a white-collar practitioner will only conduct an interview of a company witness after a comprehensive document review has been conducted. Of course, some interviews are purely fact-finding and take place in emergent situations, making pre-interview document review unlikely. However, often, the review process should be under way, or ideally, completed before interviews take place.

The key dates and types of documents (e.g., emails, phone logs, text messages and financial documents) must be determined. These parameters will be set based on the type of information sought and the interviewees to be selected.

See Chapter 11 on production of information to authorities

Cost considerations 8.8

In addition to the costs of the attorneys conducting the interviews and of support personnel such as accountants, attorney travel to and from the interview site and lodging while on site can also greatly increase the cost of an interview. To reduce travel costs, many attorneys, and especially their clients, advocate the use of videoconferencing to conduct interviews. There are some challenges to this approach. For example, if it is necessary to show a witness documents and exhibits during the interview, the logistics can be difficult. At the very least, a local company employee who is assisting in the investigation would ideally be present to produce and show the correct exhibits at the correct time, especially if the interviewer wants to keep control of the documents. It is also possible to use Webex or other online meeting programmes to share documents with witnesses during the interview when a locally based assistant cannot be present.

While using videoconferencing certainly reduces or eliminates travel costs, it can also result in a less effective interview. Conducting an interview in person

allows the interviewer to view and interpret the interviewee's attitude and body language in real time. In-person interviewing also allows the interviewer to develop a rapport with the interviewee that is usually not possible over video link. It is also likely that a witness will have a harder time being untruthful, evasive or hostile in person than to a face on a video screen. And it is much more difficult to assess an interviewee's credibility from miles away, no matter how good the high-definition screens are. The more important the interview, the more likely an in-person interview will need to be conducted. A proactive review of internal control processes is a better candidate for a telephonic or video meeting than an internal investigation designed to ferret out wrongdoing.

The best cost-control measure, though, is effective and meticulous planning. By focusing on relevant interview topics, interviews can be shortened to allow for more interviews per trip. In addition, good planning hopefully will eliminate follow-up interviews that would require additional trips.

8.9 Reporting the results of interviews

Often the format and type of report for an interview will be determined by the client in advance of any interviews. In large investigations, shorter decks or slides may be more helpful to allow the client to digest large amounts of data from various jurisdictions. These decks should include all pertinent information obtained from interviews as well as data on the number, location and type of interviews. Whether a more summarised slide deck with bullet points, or a more in-depth memo is prepared, the attorney should highlight significant findings and recommendations for next steps and further action.

Especially when preparing less detailed investigation reports, an attorney should schedule time with the client to go through the report and elaborate on key findings and recommendations. The attorney and client must be aligned on the next steps to ensure the best outcome from the investigation and interviews.

8.10 Conclusion

A well-done witness interview in a white-collar case can assist the client in determining case strategy, assessing damage, and uncovering or hopefully disproving wrongdoing. Careful scoping will ensure a focused and cost-efficient interview, and understanding at the outset what the goal of the interview is, as well as local laws and practices that might hinder attaining the goal, will avoid unnecessary hurdles and produce the result that is best for the case.

9

Co-operating with the Authorities: The UK Perspective

Ali Sallaway, Matthew Bruce, Ben Morgan and Nicholas Williams[1]

To co-operate or not to co-operate? 9.1

This chapter focuses on corporate co-operation with regulatory agencies and criminal authorities: where and when co-operation is required, its outcomes and its implications. It examines the increasing expectation that corporates should co-operate with investigations, the ever-expanding definition of 'co-operation' and factors in favour of and against it. The chapter looks at the current practice and guidance, and recent jurisprudence, with a particular focus on the meaning and application of co-operation in the context of investigations and prosecutions by the Serious Fraud Office (SFO), given that authority's clear stance that it will prosecute where the evidence allows unless corporates have genuinely and pro-actively co-operated.

Where co-operation is mandatory, the corporate has no option but to comply, or face criminal or disciplinary sanction. Examples of mandatory co-operation in the United Kingdom are:

- where there is a warrant to enter and search premises, and to seize material found therein;
- where a court issues a witness summons for a representative of the corporate to attend court, often with documents;
- where a compelled notice is issued, requiring the recipient to provide information or documents, or to attend for interview, by, for example:
    - the SFO under section 2 of the Criminal Justice Act 1987;

1 Ali Sallaway, Matthew Bruce, Ben Morgan and Nicholas Williams are partners at Freshfields Bruckhaus Deringer.

- the Financial Conduct Authority (FCA) under section 165 of the Financial Services and Markets Act 2000 where the recipient is an authorised person, or under section 168 where the recipient is any other corporate;[2] and
- the requirement that an authorised firm (or person) must disclose appropriately to the FCA and the Prudential Regulatory Authority (PRA) anything relating to the firm those regulators would reasonably expect notice of.[3]

Where co-operation is voluntary, the debate becomes more interesting. A corporate might wish to co-operate with an authority for a number of reasons. Co-operation may result in a less serious outcome, for example, a regulatory as opposed to a criminal resolution, a deferred prosecution agreement (DPA), fewer charges, less serious charges, or the period of wrongdoing under investigation being reduced. Sometimes, where an enforcement agency has an interest in a corporate, it can be beneficial to co-operate with the agency to enable it to reach an early decision to take no further action, whether for evidential, jurisdictional, public interest or other reasons. Co-operation is relevant at every stage and will even assist as mitigation in respect of sentence or sanction in the event of a successful prosecution or enforcement action.

See Chapter 39 on protecting corporate reputation

A collaborative approach may enable a corporate to manage publicity and communications in conjunction with the authority and limit reputational damage. It may also provide the opportunity to influence the course of an investigation, to avoid an overly protracted process, and to limit the cost to business that an investigation might otherwise entail. An additional benefit in the criminal sphere is the possibility of entering into a DPA, avoiding a conviction and its collateral consequences. Of course, regulatory agencies and criminal authorities will say that co-operating fully on a voluntary basis is also the right thing to do for any good corporate citizen; and while that may be true, it underestimates the myriad and sometimes competing obligations on corporates to their many stakeholders, including shareholders, employees, partners, customers and the markets generally.

9.2 The status of the corporate and other initial considerations

The status of the corporate is key. Is it a victim or witness? Is it the target or the subject of the investigation? Is it currently a witness, but circumstances indicate that it is at risk of becoming a subject? Understanding status is essential to providing proper, informed guidance.

---

2 Where it appears to the FCA that there are circumstances suggesting that a person may be guilty of one of a number of criminal offences (including insider dealing, market abuse, money laundering or certain regulatory breaches under the Financial Services and Markets Act 2000 (FSMA)), it may appoint investigators to conduct an investigation under s.168 FSMA. Once that section is invoked, the investigators assume powers under s.171, s.172 or s.173 FSMA to compel information from non-authorised persons (i.e., corporates or individuals who are not authorised or supervised by the FCA) both in the form of documents and in interview. Where a criminal investigation has commenced, the powers of compulsion are wider than where the investigation is limited to a regulatory breach.

3 Principle 11, Principles for Businesses.

At the outset, establishing the status of the corporate enables the evaluation of potential liability. Is the corporate exposed to risk? Can that risk be mitigated by co-operation? Is immunity a possibility? A consideration of these issues should define how the approach to the authority is made and how the relationship is managed.

If the corporate is a witness, it may be subject to mandatory co-operation requirements, such as compelled requests for information as outlined in Section 9.1. Witnesses face a lower expectation from prosecutors and regulators of voluntary co-operation, in terms of offering up documents and information beyond the scope of specific requests, primarily because additional co-operation offers fewer direct benefits than it might for a suspect. While proactive co-operation may enhance a corporate's relationship with its regulator or enforcement body, and be consistent with its corporate governance values, a corporate may have good reasons to be circumspect in dealings with the authorities in an investigation. In particular, a corporate witness may have an ongoing commercial relationship with the corporate suspect. This is often the case for professional advisers, such as auditors, who are frequently compelled to provide information in the context of investigations into their clients. In these circumstances, the corporate witness will have to consider its obligations to its client, and also the potential for any disclosure to expose it to regulatory investigation or litigation.

Whether a witness or a suspect, co-operation without a proper understanding of the issues and underlying facts may be difficult. Accordingly, the desire or need to co-operate may trigger an internal investigation to establish the veracity of the allegation, at least on a preliminary basis. Consideration must be given to whether the regulator or criminal prosecutor would want or expect involvement in setting the scope of an internal investigation: its subject matter, its jurisdictional and chronological reach, the sequencing of steps to gather evidence and whether it is a superficial review or a deep exploration.

See Chapter 5 on beginning an internal investigation

The corporate should be mindful of any mandatory reporting obligations that arise as its knowledge of the allegation increases. Under the Proceeds of Crime Act 2002 (POCA), 'nominated persons' in the 'regulated sector' must report to the National Crime Agency (NCA) where they have reasonable grounds for suspecting that another person is engaged in money laundering.[4] There may also be mandatory reporting or disclosure obligations that arise as matters unfold. For example, listed companies will need to consider their disclosure obligations to the market.[5]

Other initial considerations include legal privilege – invoking it where appropriate, but being sensitive to certain authorities' desire to review first accounts of witnesses.

See Chapter 35 on privilege

Where possible, the likely strength of the evidence should be assessed as quickly as possible. Information obtained by a prosecutor during an investigation

4 s.330 of the Proceeds of Crime Act 2002.

5 See Part 7 of the Financial Services Act 2012.

is generally admissible in criminal proceedings against the corporate.[6] A corporate and its advisers should, therefore, have regard to the potential impact of any documents or information they voluntarily disclose being used in proceedings against them and the extent to which voluntary co-operation may undermine any defence that the corporate later wishes to mount.

9.3 Could the corporate be liable for the conduct?

Where criminal misconduct is suspected, the extent of the corporate's involvement in, or knowledge at the time of, the alleged misconduct will be a relevant factor in whether to co-operate.

See Chapter 1, Section 1.1.1

Where the allegation is confined to an individual in a junior role, the risk of investigation and prosecution of the corporate may be low on the basis that the 'directing mind and will'[7] of the corporate was not engaged. The category of persons who fulfil that definition is narrow and, while the exact parameters are uncertain, it is usually confined to office holders, board members and very senior management – those who have the authority (whether derived from the articles and memorandum of association, or similar) to act as the corporation, rather than as its servant or agent. In these circumstances, the benefits to the corporate of voluntarily co-operating with regulatory and enforcement authorities (beyond its mandatory co-operation requirements) may be outweighed by the risks. By voluntarily identifying witnesses and documents beyond the narrow scope of the investigation, the corporate may invite the authorities to look more widely into the issues than necessary or than they otherwise would.

There are, however, some circumstances in which a special rule of attribution of liability applies – where the purpose of the legislation would be defeated if the usual hurdle to establishing corporate liability were required. The public interest in the legislation in question and the policy behind it are key to this. The court will look at the language and purpose of the statute and the particular offence to determine whose criminal act or knowledge was intended to count as that of the company. This special rule tends to be applied to administrative, regulatory or quasi-regulatory offences. Illustrative examples of offences where the court has held the special rule to apply include:

- licensing offences, including the sale of a video classified as suitable only for adults to an underage customer; the offence was committed by a company but was carried out by a member of staff;[8]

6 Material described in para. 13(6) of Schedule 17 of the Crime and Courts Act 2013 can only be used in limited circumstances but there is no limitation in the use to which other material obtained by a prosecutor during the DPA negotiation period may be put against the corporate or anyone else so far as the rules of evidence permit. See the DPA Code of Practice paras. 4.4 and 4.5 – link to Code of Practice at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/deferred-prosecution-agreements/.

7 *Tesco Supermarkets Ltd v. Nattrass* [1972] AC 153.

8 *Tesco Stores v. Brent London Borough Council* [1993] 1 WLR 1037, 1041.

- environmental offences,[9] including the creation of fraudulent records,[10] where the applicable statutory regime is a combination of offences requiring knowledge or intent and strict liability offences; and
- the requirement on a corporate to disclose its substantial holding of securities in a public issuer.[11] The individual who failed to make the disclosure was found to bind the corporate – absent that interpretation, the obligation to disclose would be rendered unenforceable.

The Court of Appeal has rejected the argument that corporate liability could be founded on a basis other than identification, based on Lord Hoffmann's opinion in the *Meridian* case. It held that the identification principles in *Tesco v. Nattrass* still stood and that Lord Hoffmann was doing no more than adapting those principles to a very specific statutory duty.[12] The supremacy of the identification principle was also reaffirmed by the Court of Appeal in the *St Regis* case.[13]

If the corporate identifies evidence to suggest that the 'directing mind and will' of the company was involved in the misconduct, or there is involvement at a lower level in the company and there is a concern that a special rule of attribution might apply, it should consider the benefits of self-reporting before the regulatory or prosecuting body itself comes to this conclusion.

In addition, 'failure to prevent' type offences (such as section 7 of the Bribery Act 2010 and Part 3 of the Criminal Finances Act 2017) will have a wider application that is not dependent on the identification principle and this should be borne in mind.[14] In a regulatory context, the liability of a firm may also be wider. A firm will, of course, have liability for acts of its employees from a regulatory perspective. And senior executives of relevant regulated firms may be held accountable through the senior managers regime, which imposes a statutory 'duty of responsibility' on those holding senior management functions within such firms – leaving them liable to enforcement action if a breach occurs on their watch.

What does co-operation mean? 9.4

Definition and descriptions 9.4.1

Co-operation with authorities in criminal cases has traditionally been in the form of a guilty plea and the offer to give evidence on behalf of the prosecution. Increasingly, co-operation is a more nuanced concept: self-reporting, saving the

9 *Alphacell Ltd v. Woodward* [1972] AC 824.

10 *Environment Agency v. St Regis Paper Co. Ltd* [2012] 1 Cr App R 177.

11 *Meridian Global Funds v. Securities Commission* [1995] 2 AC 500 PC.

12 *Attorney General's Reference (No. 2 of 1999)* [2000] 2 Cr App R 207, 217-218.

13 *Environment Agency v. St Regis Paper Co. Ltd* [2012] 1 Cr App R 177, paras. 10-11.

14 This is an expanding area of the law in England. The Criminal Finances Act 2017 introduced two new corporate offences relating to the failure to prevent the facilitation of tax evasion. In addition, in January 2017 the Ministry of Justice opened up a call for evidence on Corporate Liability for Economic Crime examining the case for reform, including the possibility of introducing further 'failure to prevent' type offences for corporates in the context of other economic crimes. At the time of writing, the outcome of the call for evidence is pending.

authority's time and resources, a willingness to cede a good deal of control of an internal investigation or hand over voluntarily relevant evidence gathered or identified, and genuine and consistent transparency are referred to by courts and authorities as key aspects of co-operation. This attitude towards co-operation was pithily summarised by SFO Director Lisa Osofsky: 'At its simplest, it's not so hard: Tell me something I don't know. Help the prosecutor find the truth. Don't obstruct, or mislead, or delay. Don't hold things back.'[15]

Under 2013 legislation,[16] a DPA is available to a designated prosecutor as an alternative to a criminal prosecution. A court-approved DPA is a method of settling a case without a conviction, where a defendant has co-operated fully with the authority. The SFO concluded its first DPA in November 2015 with ICBC Standard Bank (Standard Bank). Since then, the SFO has used this case and its subsequent DPAs to extol the virtues of voluntary co-operation.

See Chapter 23 on negotiating global settlements

In August 2019, the SFO published an extract of its operational handbook entitled Corporate Co-operation Guidance, which provides guidance to SFO prosecutors on how to assess corporate cooperation.[17] This lists several dozen 'indicators of good practice' that the SFO may take into account when assessing whether a company is genuinely co-operative. Importantly, the list is neither exhaustive nor prescriptive: the SFO acknowledges that each case will be different and a co-operating company will not necessarily display all of the enumerated conduct, or achieve a particular outcome even if it does.

As a summary of how the SFO views co-operation, the Corporate Co-operation Guidance notes:

> *Co-operation means providing assistance to the SFO that goes above and beyond what the law requires. It includes: identifying suspected wrongdoing and criminal conduct together with the people responsible, regardless of their seniority or position in the organisation; reporting this to the SFO within a reasonable time of the suspicions coming to light; and preserving available evidence and providing it promptly in an evidentially sound format.*
>
> *Genuine cooperation is inconsistent with: protecting specific individuals or unjustifiably blaming others; putting subjects on notice and creating a danger of tampering with evidence or testimony; silence about selected issues; and tactical delay or information overloads.*[18]

The guidance is considered in detail further below.

15 Speech by Lisa Osofsky, SFO Director, at the 35th International Conference on the Foreign Corrupt Practices Act in Washington, DC, 28 November 2018 (https://www.sfo.gov.uk/2018/12/04/keynote-address-fcpa-conference-washington-dc/).

16 Crime and Courts Act 2013.

17 SFO Operational Handbook, Corporate Co-operation Guidance (https://www.sfo.gov.uk/download/corporate-co-operation-guidance/).

18 Ibid., p.1.

Genuine and continual co-operation 9.4.2

Authorities expect co-operation to be genuine, proactive and continual. For the FCA, a firm's pattern of co-operation over the period leading up to the investigation, as well as during the investigation itself, is relevant. The FCA Handbook notes that:

> *An important consideration before an enforcement investigation and/or enforcement action is taken forward is the nature of a firm's overall relationship with the FCA and whether, against that background, the use of enforcement tools is likely to further the FCA's aims and objectives. So, for any similar set of facts, using enforcement tools will be less likely if a firm has built up over time a strong track record of taking its senior management responsibilities seriously and been open and communicative with the FCA.*[19]

The Office of Fair Trading (OFT) is the predecessor to the Competition and Markets Authority (CMA) and adopted a similar approach with regard to cartel investigations. The OFT has stated that one condition for leniency is that '[t]he applicant must maintain continuous and complete co-operation throughout the investigation and until the conclusion of any action (including criminal proceedings and defending civil or criminal appeals) by the OFT arising as a result of the investigation'.[20]

Further, the Office of Financial Sanctions Implementation (OFSI) within HM Treasury, which has powers to impose potentially significant monetary penalties on companies and individuals for breaches of financial sanctions law, has noted in its guidance: '[If] we discover that parties have dealt with us in bad faith and if the case is not criminally prosecuted, we will normally impose a monetary penalty.'[21]

In the criminal sphere, both co-operation and remorse are mitigating features for which a defendant can expect a reduction in sentence. Where a DPA is under consideration, the key public interest factor against prosecution is co-operation: considerable weight will be given to a 'genuinely proactive approach adopted by [an organisation]'s management team when the offending is brought to their notice'.[22] Whether a DPA is in the public interest is a focus of the court in its

19 FCA Handbook, EG 2.12.1.

20 Para. 2.7(c) of 'Applications for leniency and no-action in cartel cases', guidance document OFT1495, July 2013 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284417/OFT1495.pdf). The CMA Board has adopted this guidance and references to OFT should be read as to the CMA, which has been retained unamended but does not take account of developments since its publication (see https://www.gov.uk/government/publications/leniency-and-no-action-applications-in-cartel-cases).

21 'Monetary penalties for breaches of financial sanctions – guidance', OFSI, April 2017 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/605884/Monetary_penalties_for_breaches_of_financial_sanctions.pdf).

22 DPA Code of Practice, para. 2.8.2.

assessment of the proposed agreement. As such, it is unsurprising that the SFO's expectations of continual co-operation are so high where a DPA is in play.

Co-operation will clearly be considered in the round, by reference to the company's broader attitude towards the investigation. Companies that make incorrect or unsubstantiated arguments about the underlying nature of the misconduct run a real risk of being deemed unco-operative, a point highlighted by the conduct of Sweett Group: the company was heavily criticised by the SFO and the court for apparently attempting to deliberately mislead the SFO, by attempting to obtain a letter characterising the offending payment its subsidiaries had made as a legal finder's fee under United Arab Emirates law.[23] On the other hand, companies that co-operate fully with the SFO can earn significant leniency. For example, in the *Rolls-Royce* case, the SFO offered, and the court approved, a DPA with a 50 per cent discount to the monetary penalty that would otherwise have been required. This represented the one-third discount that is the equivalent of what is usually available for an early guilty plea plus an additional 16.7 per cent discount in recognition of Rolls-Royce's 'extraordinary cooperation'.[24] The SFO has also agreed DPAs with Tesco Stores Limited, Serco Geografix Ltd and Sarclad Limited that all involved a 50 per cent discount to the monetary penalty.

Of further interest to corporates is the approach to co-operation taken by the Information Commissioner's Office (ICO). The ICO, like the SFO and FCA, will take the level of co-operation provided by companies into account when considering enforcement. In considering any penalty, failure to cooperate with an ICO investigation will be considered an aggravating factor.[25] An instructive example of the ICO's tough approach is the £400,000 fine and criminal penalty handed to Keurboom Communications after Keurboom failed to comply with an information notice regarding a breach of the Privacy and Electronic Communication Regulations.[26]

See Chapter 40 on data protection

9.4.3 Prompt reporting to the SFO

A corporate should report to the SFO as promptly as possible, if it wishes to be considered as co-operating. How early a corporate self-reports is a factor the SFO may consider when deciding to offer a DPA.[27] This does not mean that corporates should report all allegations of criminal behaviour as soon as they become aware of them.[28] The corporate will need to consider and verify such allegations to a certain extent before deciding whether it is necessary and appropriate to take the

23 *R v. Sweett Group*, Sentencing Remarks.

24 *SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 19.

25 ICO, Draft Regulatory Action Policy (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf), pp. 24 and 28.

26 See ICO Monetary Penalty Notice to Keurboom Communications Ltd (https://ico.org.uk/media/action-weve-taken/enforcement-notices/2014013/mpn-keurboom-ltd-20170503.pdf).

27 DPA Code of Practice, para. 2.9.2.

28 Speech by Lisa Osofsky, SFO Director, at the Royal United Services Institute in London, 3 April 2019 (https://www.sfo.gov.uk/2019/04/03/fighting-fraud-and-corruption-in-a-shrinking-world/).

serious step of reporting itself to the SFO. Reporting wrongdoing but failing to verify it, or reporting it knowing or believing it to be inaccurate, misleading or incomplete, is a factor in favour of prosecution.[29] What level of investigation is required to 'verify' wrongdoing is undefined. This is a judgement for the corporate to make with assistance from its advisers. The following factors should be taken into account:

- where possible, the alleged criminal conduct should be reported to the SFO before it otherwise becomes aware of it. As such, the corporate should be alert to the possibility of whistleblowers or other organisations or individuals (e.g., NGOs) approaching the SFO, and should be conscious of the implications of any other reports that the corporate may have made to other authorities in the United Kingdom or overseas;
- the corporate is entitled to conduct an 'initial assessment' of the allegation but as soon as reasonable grounds to suspect wrongdoing in the way the company or those associated with it conduct business[30] are identified, they should be flagged to the SFO; and
- the extent to which a company involves the prosecutor in the early stages of an investigation is a relevant factor in assessing a company's co-operation.[31]

In the case of Standard Bank, the bank reported the alleged misconduct 'within a matter of days of it coming to its attention',[32] and, in passing sentence on the bank, the court noted that considerable weight was to be attached to the fact that it had 'immediately reported itself to the authorities and adopted a genuinely proactive approach to the matter'.[33] However, it seems likely that Standard Bank had mandatory reporting obligations under POCA given that the bank's solicitors had reported the matter to the Serious Organised Crime Agency (which was subsequently merged into the NCA) six days before the bank reported the matter to the SFO.[34]

In the case of Sarclad, a global programme designed to improve compliance in the relevant subsidiary unearthed concerns about specific contracts; as a result, Sarclad took immediate action by retaining a law firm to undertake an independent internal investigation.[35] Within a month of commencing the investigation, the law firm had informed the SFO that a self-report might be forthcoming. Six weeks later, the lawyers met with the SFO to confirm that Sarclad would

29 DPA Code of Practice, para. 2.8.1(vi).

30 See, for example, Lisa Osofsky's speech of 3 April 2019.

31 See paragraph 2.9.2 of the DPA Code of Practice.

32 *SFO v. Standard Bank plc,* Statement of Facts prepared pursuant to para. 6(1) of Schedule 17 to the Crime and Courts Act 2013, para. 4.

33 *SFO v. Standard Bank plc*, Approved Judgment,(Case No. U20150854) [2016] Lloyd's Rep FC 102, para. 27.

34 Press release entitled 'SFO agrees first UK DPA with Standard Bank', 30 November 2015 (https://www.sfo.gov.uk/2015/11/30/sfo-agrees-first-uk-dpa-with-standard-bank/).

35 *SFO v. Sarclad Ltd*, Approved Judgment, (Case No. U20150856) [2016] 7 WLUK 220; [2016] Lloyd's Rep FC 509, para. 11.

be making a self-report at the conclusion of the investigation. This was supplemented by continuing assistance and two further reports. The court commended 'the promptness of the self-report, the fully disclosed internal investigation and co-operation of Sarclad'.[36]

A corporate is unlikely to get credit from the SFO for self-reporting where there is a sense that its hand has been forced, as was the case with the Sweett Group, who apparently only reported the conduct at issue to the SFO following a tip-off from the *Wall Street Journal* that it was about to publish a story.[37]

Likewise, a cartel member reporting and providing evidence of a cartel will not benefit from leniency if, for example, the CMA is already investigating the cartel, or if another cartel member reported the wrongdoing beforehand.[38]

In the absence of a self-report, a corporate will likely need to demonstrate a much greater level of subsequent co-operation to earn a comparable degree of leniency from the SFO. In the case of Rolls-Royce, the SFO acknowledged that the initial investigation was not triggered by a self-report. Even so, the 'extraordinary' co-operation offered by Rolls-Royce persuaded the SFO and the court not to 'distinguish between its assistance and that of corporates who have self-reported from the outset.' This was largely due to the fact that what Rolls-Royce subsequently reported during the course of the investigation was 'far more extensive (and of a different order)' than would have otherwise been exposed without the co-operation Rolls-Royce provided.[39]

9.4.4 Conducting an SFO-approved internal investigation

Once a self-report has been made, the SFO expects genuine and constructive co-operation. This means that, following a self-report, any internal investigation conducted by the corporate or its advisers should be done in conjunction with the SFO and with its approval.[40] The SFO will want to have a reasonable degree of involvement in the early stages of an internal investigation – to enable it to discuss work plans and timetabling and to give directions, for example relating to data capture and processing.[41] The SFO will also expect a co-operating company to 'consult in a timely way with the SFO before interviewing potential witnesses or suspects, taking personnel/HR actions or taking other overt steps'.[42]

36 Ibid., para. 16.

37 Speech by Camilla de Silva, Joint Head of Bribery and Corruption at the SFO, at ABC Simple Minds Financial Services conference on 15 March 2018: 'the sooner you come in, self report and the more you are open with us, the more you have to be rewarded for.'

38 Para. 2.9 of 'Applications for leniency and no-action in cartel cases', guidance document OFT1495, July 2013 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284417/OFT1495.pdf).

39 *SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 22.

40 DPA Code of Practice, para. 2.9.2.

41 Ibid., para. 2.9.2.

42 Corporate Co-operation Guidance.

SFO expectations on data handling 9.4.5

The SFO is particularly concerned that relevant data is properly preserved. For example, its Corporate Co-operation Guidance advises companies to ensure that the digital integrity of material is preserved; to identify the reasons for any data loss, deletion or destruction; and to create and maintain an audit trail on the acquisition and handling of data including digital material and devices, hard copy files and financial material. While this standard is already well known to global companies, preserving the integrity of data (and later collecting it) may require a significant effort. Companies may consider evaluating, in advance of any investigation, what data sources they have, how data is preserved and stored and over what period, and how it can be accessed at a later date.

The SFO Corporate Co-operation Guidance notes co-operation may involve providing material from overseas where it is in the possession or under the control of the organisation and identifying and facilitating access to data held by third parties.

The assistance provided by Standard Bank, for example, included providing shared documents collected from email servers held in Africa, inboxes, hard drives and shared drives, paper files, CCTV images recorded in Africa and recordings of telephone conversations. The SFO would not have had access to much of this evidence had it not been provided voluntarily by the bank.[43] Similarly, Sarclad identified and provided relevant information that extended the investigation beyond the SFO's original scope. Email caches were volunteered.[44] Rolls-Royce agreed to provide the SFO with unfiltered access to its records – some 30 million documents – and permitted the SFO to conduct its own digital review to identify potentially privileged documents with any issues of privilege to be resolved by an independent counsel.[45]

Facilitating SFO access witnesses 9.4.6

The SFO is particularly concerned that 'first accounts' from witnesses are not prejudiced.[46] Other regulatory and enforcement authorities, including the FCA, are increasingly adopting a similar stance.

See Chapter 3 on self-reporting to authorities

From a prosecutor's perspective, achieving best evidence is a key principle in a criminal prosecution. The first account of a witness is crucial, and the circumstances in which it is obtained can be critical to the credibility and efficacy of the evidence in a trial. Discrepancies between a first account and subsequent testimony can undermine the prosecution case. As such, the SFO places particular significance on obtaining first access to witnesses, or to notes or summaries of

43 *SFO v. Standard Bank plc,* Statement of Facts prepared pursuant to para. 6(1) of Schedule 17 to the Crime and Courts Act 2013, para. 4.

44 *SFO v. Sarclad Ltd*, Approved Judgment, (Case No. U20150856) [2016] 7 WLUK 220; [2016] Lloyd's Rep FC 509.

45 *SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249.

46 DPA Code of Practice, para. 2.9.3.

first accounts.[47] Many defence lawyers would take a different view, arguing that first accounts are not as helpful and reliable, and therefore not as critical, as the SFO maintains. Nonetheless, a failure to co-operate with the SFO in this regard could jeopardise the offer of a DPA.[48] In certain circumstances, the SFO or the FCA may expect corporates not to interview witnesses before consulting with them,[49] or they may request that a company does not interview potential witnesses before a compelled interview has been carried out or a witness statement obtained. Where a corporate is able to interview witnesses, the SFO or the FCA may wish to dictate the order in which interviews are carried out, see materials or questions to be put to witnesses and receive copies of any work-product generated following each interview.

The SFO will also expect co-operating companies to make employees and (where possible) agents available for SFO interviews, including arranging for them to return to the United Kingdom if necessary and identifying third parties to interview.

9.4.7 Privilege and the SFO

The legal professional privilege often claimed to protect from disclosure communications generated during the course of an investigation has been an area of focus for the SFO in recent years, particularly in relation to interview notes. Public statements by the SFO make clear that it considers as a 'significant mark of co-operation a company's decision' to waive privilege over notes of witness interviews.[50] Rolls-Royce received credit for voluntarily disclosing, with limited waiver of privilege, memoranda from over 200 interviews conducted as part of its internal investigation.[51]

Standard Bank on the other hand is understood not to have provided notes (or referred to first-account witness interviews in its internal investigation report to avoid waiving privilege). Instead, it provided oral summaries. The same was true

47 See, for example, Alun Milford's speech of 29 March 2016: 'Why are witness first accounts so important to us? The immediate point is that they simply help us understand quickly what went on. Of course we can and we will go to speak to witnesses ourselves but companies who tell us what they were told during the course of an internal investigation plainly help us in the course of our inquiries. There is a second reason why we want witness accounts. As I have previously made clear, people who give an account to an internal investigation are liable to be witnesses in any criminal case we might bring. In considering the evidence witnesses might give us, we are duty-bound to assess its accuracy and integrity. So fundamental to prosecutors is that duty that it is set out in the Code for Crown Prosecutors. An important way in which accuracy or integrity is tested is by reference to first accounts. Plainly, if we do not have first accounts then our ability to assess witness credibility might be affected to the extent that we might not be able to call them as witnesses.'

48 DPA Code of Practice, para. 2.9.2.

49 Corporate Co-operation Guidance, Preserving and providing material, para. 6(i). Further, the court in *SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 20(i) cited Rolls-Royce's deferring of internal interviews until the SFO had first completed its interview as evidence of their co-operation with SFO.

50 See Lisa Osofsky's speech of 3 April 2019.

51 *SFO v. Rolls-Royce* (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 20(ii).

of Sarclad Ltd. However, the decision in *R(AL) v. SFO*[52] demonstrates the difficulties that can arise for the SFO from this approach.

In *R(AL) v. SFO*, a former employee of Sarclad Ltd, a defendant in related criminal proceedings, brought a claim for judicial review to challenge the SFO's decision not to require production of witness interview notes, over which the company claimed privilege. The High Court ultimately dismissed the claim since the claimant had not exhausted all available remedies before the Crown Court. However, the Court also made plain its view that the SFO had not complied with its duty, as a prosecuting authority, to take further steps to obtain witness interview notes so that they may be disclosed in the criminal proceedings against the individual in accordance with the defendant's right to a fair trial under Article 6 of the European Convention on Human Rights. In that case, the Court noted that it was not sufficient for the SFO to apply a 'not obviously wrong' test to examining a company's claims to privilege and its 'duty is to assess claims for privilege properly and not cursorily and superficially'.

This case follows other high-profile decisions in the English courts in relation to interview notes. For example, in the 2016 case *The RBS Rights Issue Litigation*,[53] the High Court rejected a claim of legal advice privilege over memoranda of employee interviews prepared by the bank's lawyers. 'Client' for the purposes of legal advice privilege was interpreted, by reference to *Three Rivers District Council v. Governor of the Bank of England*,[54] to cover only those individuals authorised to seek and receive advice from the lawyers. The employees interviewed by the lawyers were not, therefore, considered to be 'clients' of the bank's lawyers.[55] Based on the evidence available to it, the court also rejected the bank's claims that the notes in question were subject to legal advice privilege on the basis that they comprised lawyers' working papers.

Further, in *Director of the SFO v. ENRC*, the SFO initially successfully challenged claims of privilege over various documents produced during ENRC's internal investigation and subsequent engagement with the SFO.[56] But this decision was overturned on appeal on the basis that the interview notes and other materials (including the work-product of forensic accountants) were protected by litigation privilege.[57] Notably, the Court of Appeal found that criminal proceedings were sufficiently contemplated for litigation privilege purposes at the point at which ENRC commenced an internal investigation following a whistleblower report alleging corruption in parts of its business, and they were certainly contemplated when the SFO subsequently contacted ENRC about the same matter (even though the SFO stated it was not, at that time, carrying out a criminal investigation into ENRC). On the question of legal advice privilege, the Court of

52 *R(AL) v. SFO* and others [2018] EWHC 856 (Admin).

53 *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch).

54 *Three Rivers District Council v. Governor of the Bank of England* [2001] UKHL 16.

55 *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch).

56 *SFO v. ENRC* [2017] EWHC 1017 (QB) (8 May 2017).

57 *Serious Fraud Office v. Eurasian Natural Resources Corporation* [2018] EWCA Civ 2006.

Appeal clearly indicated that it considered the narrow definition of the 'client' as established in *Three Rivers No. 5* to be outdated, and that it would have departed from that decision if it had been able to do so.

Although the decision of the Court of Appeal in *SFO v. ENRC* may give a company engaging with the SFO greater comfort when asserting litigation privilege over investigation documents, companies seeking a resolution will still need to consider if it is in their strategic interests to waive privilege (on a limited basis) in such documents. As a matter of principle, maintaining privilege should be a 'neutral' factor as far as obtaining credit for co-operation is concerned. Privilege is a fundamental right. The DPA Code of Practice recognises that there is nothing in the existence of the DPA process that alters that right.[58] However, the Court of Appeal in *ENRC* did note that an examination of a company's co-operation, for the purposes of determining whether a DPA would be in the interests of justice, 'will consider whether the company was willing to waive any privilege attaching to documents produced during internal investigations, so that it could share those documents with the SFO'. In light of this, the SFO may, in practice, consider it to be a positive sign of co-operation if a company chooses to waive privilege in certain documents for the purposes of assisting the SFO in its investigation. On 2 October 2018, the SFO announced that it would not be seeking to appeal against the Court of Appeal's decision.

See Chapter 35 on privilege

In light of these developments over recent years, the Corporate Co-operation Guidance focuses, in large part, on privilege. The language of the guidance is particularly strong on this point, signalling the SFO is continuing its robust stance and willingness to test claims of privilege over internal investigation materials. The guidance establishes two new procedural expectations for companies seeking to assert privilege: first, to provide certification by independent counsel supporting any claim of privilege, and second, to provide 'privilege logs' itemising each document withheld on the basis of privilege and the basis on which each is privileged. These new procedures would, if implemented, generally make asserting privilege meaningfully more time-consuming and expensive. At the same time, they may also signal that, if these procedural steps are taken, there is a clearer path for a company to assert privilege while maintaining a co-operative stance.

The Corporate Co-operation Guidance also reiterates the SFO's previous DPA Code of Practice in providing that, when the SFO is considering a company's co-operation for the purposes of deciding whether to offer a DPA, it will expect the company to disclose 'witness accounts' and documents shown to witnesses.[59] The DPA Code of Practice did not specify what the SFO meant by 'witness accounts' – and in some of the DPA cases the SFO accepted summaries of discussions with witnesses (including 'oral proffers') as sufficient for these purposes. But the Corporate Co-operation Guidance now adds a new express expectation that companies seeking co-operation credit should also provide any recordings, notes

58 DPA Code of Practice, para. 3.3.

59 DPA Code of Practice, para. 2.8.2(i).

and transcripts of witness interviews and identify a witness competent to speak about the contents of each interview.

The SFO states that companies that retain a legitimate claim to privilege over such witness material will not be penalised for asserting that claim (where backed up by an independent certification). That said, it is not yet clear whether the SFO will expect such companies to work harder in other areas to 'make up' for the lack of credit they would have otherwise received for disclosing privileged materials.

The SFO has elsewhere made clear that in evaluating the quality of a company's co-operation, it will view the waiver of privilege as a 'strong indicator of co-operation' and an 'important factor' in deciding whether to offer a DPA.[60] Some will undoubtedly question whether the distinction the SFO has drawn in this context is meaningful. Companies facing the threat of prosecution may question if there is a practical difference between failing to achieve a credit and being penalised.

Highlighting exculpatory material to the SFO 9.4.8

In recent years, the SFO has emphasised the importance of holding individuals accountable for criminal behaviour. The Corporate Co-operation Guidance repeats this overarching objective in its introductory remarks. It also articulates a new and controversial expectation that a co-operative company will also assist the SFO in identifying documents or information capable of assisting a potential accused or undermining the case for the prosecution (typically called 'exculpatory material'). This may be a result of the criticisms the SFO faced last year in the case of *R(AL) v SFO*.[61] In that case, the English High Court made plain its view that the SFO had not complied with its duty, as a prosecuting authority, to take steps to obtain relevant materials (in that case interview notes) so that they could be disclosed in the criminal proceedings against an individual in accordance with the defendant's right to a fair trial under Article 6 of the European Convention on Human Rights. The extent to which this expectation places a new burden on co-operating companies remains to be seen.

In practice, the overall level of co-operation requested by the SFO in its Corporate Co-operation Guidance may feel uncomfortable for a corporate – particularly one not in a regulated sector – unfamiliar with regulatory oversight. Some practitioners would argue that there should be a curb on the extent of the co-operation expected by the SFO and that corporates should do what they are legally required to do and thereafter exercise careful judgement as to the merits of co-operating further (e.g., there may be risks in identifying and providing material beyond what is sought through mandatory requests).

60 Speech by Lisa Osofsky, Director of the SFO, on 3 April 2019.

61 *R. (on the application of AL) v. Serious Fraud Office* [2018] EWHC 856 (Admin).

9.5 Co-operation can lead to reduced penalties

Co-operation with authorities in criminal cases has always been rewarded with a more lenient outcome for a defendant: whether through the statutory recognition that a sentence should be reduced for a guilty plea at the earliest opportunity (the current guideline being a reduction of one-third),[62] through the passing of a less onerous type of sentence (a non-custodial as opposed to a custodial sentence), or through a lower multiplier being used to calculate a fine for a corporate. Conversely, attempts to conceal misconduct will be taken into account and result in a more severe sentence.[63]

Individuals who plead guilty and offer significant voluntary co-operation with a prosecutor, may be entitled to a lesser sentence under section 73 of the Serious Crime and Police Act 2005 (SOCPA).[64] A defendant enters into an agreement with the authorities under SOCPA to provide certain assistance, the extent and nature of which is taken into account when he or she is sentenced. The assistance is often directed at obtaining evidence about other individuals, or establishing facts that advance the investigation. This approach is being used increasingly in fraud and organised crime cases. It has been used effectively by the FCA and has resulted in defendants avoiding immediate sentences of imprisonment.[65]

The likelihood of prosecution and the likely sanction in the event of conviction are important factors in any decision voluntarily to co-operate with an investigation by a regulatory or enforcement body. This is primarily because there is no guarantee that voluntary co-operation will result in a reduced sanction or complete immunity. The corporate and its advisers should not lose sight of the fact that, where there are allegations that criminal offences or regulatory breaches have been committed, the regulatory and enforcement bodies' primary role is to properly investigate and prosecute or otherwise sanction the offender.

The more serious the offence, the less likely it is that a DPA (as opposed to prosecution) will be considered to be in the public interest. However, in the *Rolls-Royce* case, the court acknowledged that, notwithstanding the gravity of the wrongdoing committed by Rolls-Royce, on the right terms it was in the interests

62 s.144 Criminal Justice Act 2003, and the Sentencing Council Definitive Guideline on Reduction in Sentence for a Guilty Plea. See also Attorney General's Guidance on the acceptance of pleas: https://www.gov.uk/guidance/the-acceptance-of-pleas-and-the-prosecutors-role-in-the-sentencing-exercise.

63 See, for example, 'Fraud, Bribery and Money Laundering Offences Definitive Guideline' 1 October 2014, p. 50. (See also Chapter 25 on fines, disgorgement, etc.).

64 This applies where an offence specified under the Schedule to SOCPA has been committed. Prosecutors holding SOCPA powers include the CPS, FCA and SFO. See also CPS Guidance on SOCPA: http://www.cps.gov.uk/legal/s_to_u/socpa_agreements_-_note_for_those_representing_assisting_offenders/.

65 For example, *R v. Anjam Ahmed*; sentencing hearing at Southwark Crown Court, 22 June 2010; a SOCPA agreement was in place resulting in a suspended, rather than immediate, term of imprisonment. (See also Chapter 25 on fines, disgorgement, etc.).

of justice to resolve the conduct by way of a DPA rather than a trial.[66] The legislation requires any financial penalty that forms part of a DPA (the 'meat' of the sentence for a company) to be broadly comparable to a fine the court would have imposed following a guilty plea.[67] However, in *SFO v. Sarclad Ltd*, Sir Brian Leveson, President of the Queen's Bench Division, allowed a 50 per cent discount 'given that the admissions are far in advance of the first reasonable opportunity' and therefore represented additional mitigation.[68]

Similarly, in *SFO v. Rolls-Royce*, a discount of 50 per cent was allowed because Rolls-Royce had demonstrated 'extraordinary cooperation'.[69] This discount comprised a discretionary 16.7 per cent discount in recognition of Rolls-Royce's co-operation, in addition to the one-third discount that is normally available as part of a DPA.[70] This discount was considered appropriate even in circumstances where Rolls-Royce was accused of corrupt practices spanning 24 years in seven countries. Rolls-Royce's co-operation, however, was extensive, including close co-operation with the SFO over the conduct of its internal investigations, granting the SFO full prior access to documents and witnesses, consulting with the SFO over media coverage, and waiving privilege over documents connected to the internal investigation. In addition, Rolls-Royce had taken considerable steps to reform its anti-bribery corruption compliance programme. Various examples of this co-operation by Rolls-Royce were detailed by Leveson P as justification for approving the terms of the DPA, who stated he was satisfied that Rolls-Royce 'could not have done more to have exposed its own misconduct'.[71]

Serco Geografix Ltd (SGL) also received a 50 per cent discount off the penalty as part of its DPA with the SFO. SGL's co-operation included assisting the SFO's criminal investigation by appointing independent lawyers to carry out a document review and provide a report to the SFO, granting the SFO unrestricted access to employee emails and waiving privilege over certain documents. The parent company, Serco Group PLC's co-operation further entailed a full change of senior management, extensive internal and external auditing and the putting in place of a corporate renewal programme aimed at improving operating practices. This DPA was notable for being the first in which a parent company took on undertakings that attached to the now dormant subsidiary. Mr Justice Davis looked to non-binding precedent when calculating the penalty and discount, noting: 'In all but one of the earlier instances of approval of DPAs the financial

66 *SFO v. Rolls-Royce*, Approved Judgment, (Case No. U20170036) [2017] Lloyd's Rep FC 249, paras. 61-64.

67 Crime and Courts Act 2013, Schedule 17, para. 5(4).

68 *SFO v. Sarclad Ltd*, Approved Judgment, (Case No. U20150856) [2016] 7 WLUK 220; [2016] Lloyd's Rep FC 509, para. 57.

69 *SFO v. Rolls-Royce*, Approved Judgment, (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 121.

70 See Appendix B, *SFO v. Rolls-Royce*, Approved Judgment, (Case No. U20170036) [2017] Lloyd's Rep FC 249.

71 *SFO v. Rolls-Royce*, Approved Judgment, (Case No. U20170036) [2017] Lloyd's Rep FC 249, para. 38.

penalty has been discounted by 50% rather than the one third . . . required by the Sentencing Council.'[72] The judge justified this by noting that DPAs save resources with regard to investigation and prosecution and that significant fine reductions encourage early self-reporting of corporate crime.

Tesco Stores Limited also obtained a 50 per cent reduction on the monetary penalty as part of its DPA.

In light of this string of recent cases, it would appear that companies seeking DPAs should expect at least a 50 per cent discount in return for broad and effective co-operation.

In the regulated space, co-operation can also lead to reduced penalties. Although regulated firms and individuals are required to co-operate with the FCA, the authority makes clear that proactive co-operation can benefit individuals or firms in a number of ways: this can include not pursuing enforcement action,[73] reduced charges or lighter sanctions being sought (something which may ultimately be reflected in the final notice). The FCA's Enforcement Guide makes clear that the settlement discount scheme allows a reduction in a financial penalty or period of suspension, restriction or condition that would otherwise be imposed, if agreement is reached at an early stage. Co-operation appears to be becoming ever more important. FCA procedure allows a firm to settle aspects of a case and achieve a discount in respect of those aspects, while continuing to contest other aspects of the case. Timetables for settlement discussions will be set for efficiency and effectiveness and the FCA will expect firms and others to give it all reasonable assistance in this regard.

In the competition context, cartel members who self-report and provide information about the cartel can benefit from the CMA's leniency regime. To do so, they must be the first member to report the cartel and must do so before the CMA commences an investigation of its own volition. They must also fulfil certain immunity conditions, which include maintaining continuous and complete co-operation throughout the investigation and refraining from further participation in the cartel activity.[74]

Equally, the OFSI within HM Treasury, which may impose potentially significant monetary penalties on companies and individuals for breaches of financial sanctions law, has published guidance that indicates that timely, voluntary and materially complete disclosure, made in good faith, will be a key mitigating factor when it is deciding the level of any penalty (including a potential penalty reduction of up to 50 per cent).[75]

---

72 S*FO v. Serco Geografix Ltd*, Approved Judgment, (Case No. U20190413) [2019] 7 WLUK 45, para 39.

73 See FCA Handbook, EG 2.1.4.

74 https://www.gov.uk/guidance/cartels-confess-and-apply-for-leniency and https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284417/OFT1495.pdf.

75 'Monetary penalties for breaches of financial sanctions – guidance', OFSI, April 2017 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/605884/Monetary_penalties_for_breaches_of_financial_sanctions.pdf).

Other options besides co-operation 9.6

In circumstances where no regulator or enforcement body is yet involved in, or aware of, an issue, whether to co-operate at all (i.e., whether to self-report) remains a judgement call for a corporate taking into account the factors described earlier.

Once a regulator or enforcement body is on the scene, co-operation in its various forms may, as described above, afford significant advantages for a corporate. However, there is still a balance to be struck.

On the one hand, it is important that a corporate does not entirely prostrate itself where that is not warranted, that it constantly keeps under review whether the investigating or prosecuting authority has a provable case, and that it does not admit to facts or enter pleas that it has committed wrongdoing without advice. If the corporate is on reasonable grounds evidentially, it may be well advised to maintain a robust stance in the course of an investigation and even to defend the case at trial. Moreover, other factors may impact the nature and extent of the co-operation that the corporate is prepared, or able, to entertain. For example, some aspects of the voluntary co-operation that an investigative or enforcement authority might expect could be problematic for a corporate where follow-on litigation is pending or threatened, and many corporates will be unwilling to be seen to abandon current or former employees who are themselves under scrutiny and to co-operate in their investigation and prosecution.

On the other hand, where the risk of a conviction (and its potential collateral consequences) cannot be entirely excluded, a guilty plea or a DPA may be more attractive. A DPA will only be available where a corporate is deemed to have been sufficiently co-operative, and, for both pleas and DPAs, the extent of the corporate's co-operation will impact the sentencing or the fine. However, in the bribery space at least, the outcomes of the guilty plea in the *Sweett Group* case and the DPA in the *Standard Bank* case (both involving large fines with similar percentage reductions) have led commentators to consider whether fines would have been materially different in the event of a conviction after a trial. Also, a DPA is likely to include terms requiring co-operation with ongoing prosecutions and continuing disclosure obligations in respect of relevant matters (as seen with the DPAs in the *Standard Bank* case,[76] the *Sarclad Ltd* case and the *Rolls-Royce* case). The extent of this ongoing duty was considered, in part, in *R(AL) v. SFO*. In that case the court criticised the SFO for failing to seek to use Sarclad Ltd's duty of co-operation under the terms of the DPA to require it to disclose to the SFO certain witness interview notes (Sarclad Ltd had refused on the grounds that, it claimed, the notes were privileged). The court also criticised the SFO for failing to consider whether it should require a waiver of such privilege (to the extent any attached to the notes) as part of the duty of co-operation.

The position of individuals connected to alleged corporate wrongdoing is another factor practitioners consider carefully when assessing the merits of

76 Deferred Prosecution Agreement between Standard Bank PLC (now ICBC Standard Bank PLC) and the Serious Fraud Office (https://www.sfo.gov.uk/cases/standard-bank-plc/).

co-operation or the desirability of a DPA as opposed to a guilty plea. If the individuals whose alleged misconduct forms the basis of the case against the companies are not routinely charged or successfully prosecuted, that will become a factor corporates will have to take into account in their assessment of the overall exposure to risk.

9.7 Companies tend to co-operate for a number of reasons

With all of that said, corporates increasingly choose to co-operate with regulators and enforcement bodies, in some cases very extensively. In some cases, this is just a matter of being a good corporate citizen and maintaining integrity and credibility in the eyes of stakeholders, government and the general public. Sometimes there will be considerable stakeholder pressure (e.g., from a new board or shareholders). Sometimes there is an ongoing relationship with the investigating authority to think about.

In other cases, there may be significant strategic benefits to co-operating. Without some degree of co-operation, a corporate will have little control over, or ability to influence, a regulatory or criminal investigation. Co-operation will often mean the company has a better view of the investigation and a greater degree of communication with the investigating authority, and these may provide an opportunity to influence the course of the investigation, to offer up mitigation to adverse findings immediately and even to effect the discontinuance of an investigation. Co-operation that is thorough and genuine throughout may help resolve the issue in a non-adversarial way (such as through a DPA), while retaining some control over what, if any, admissions are made and what is said publicly by the relevant authority.[77]

Certainly, few corporates will take lightly the financial implications of a prolonged investigation or the management time and business interruption it will entail. Nor can corporates afford to be dismissive of the impact a drawn-out process will have on the morale of employees and the risk of 'talent flight'. For many companies and their stakeholders, gaining clarity and certainty and being able to return to focusing on their day-to-day business will be an absolute priority.

77 A DPA is not, however, guaranteed, even for companies that co-operate. In *R v. Skansen*, a case prosecuted by the CPS in March 2018, the corporate defendant – which was by then dormant – was convicted, following a trial under section 7 of the UK Bribery Act. The company had demonstrated co-operation having investigated and self-reported conduct to the police that might not otherwise have come to light, and co-operating with the police and CPS. However, a DPA was not offered. The judge questioned why a prosecution was being brought against a dormant company against whom it was agreed that no financial penalty could be imposed and whose only sentence could be an absolute discharge. The status of the company, and a desire to send a deterrent message appear to have been the reasons: the CPS said that the public interest test for a prosecution was satisfied so that a message could be sent to others in the industry and they had decided that no ongoing benefit could be achieved by a DPA. The SFO has brokered four DPAs to date, while the CPS has not agreed any. This case is a reminder that a DPA is by no means a predictable outcome – particularly with agencies other than the SFO – even where co-operation exists.

Finally, no company will relish the prospect of a criminal conviction and the reputational impact this will have; and for many companies, there may be broader implications of a criminal conviction, such as debarment from public tendering, that outweigh the narrow legal merits of challenging allegations of wrongdoing.

Multi-agency and cross-border investigations 9.8

Overview 9.8.1

The ways regulators and criminal prosecutors choose to co-operate with each other are numerous and varied. There is undoubtedly an increasing desire for agency co-operation on domestic and international levels.

The extent of co-operation between regulators typically only becomes apparent in the event of public resolution of any wrongdoing.[78] For example, in the context of the 2017 *Telia* case, the DOJ noted the valuable assistance of law enforcement colleagues in 13 jurisdictions, including the United Kingdom, in investigating the matter.[79] In December 2014, the US authorities fined the US division of French infrastructure giant Alstom US$772 million in respect of bribery offences, and expressly acknowledged the assistance received from authorities in Indonesia, Switzerland, the United Kingdom, Germany, Italy, Singapore, Saudi Arabia, Cyprus and Taiwan, and the World Bank during their investigation.[80] The SFO commenced its own investigation into Alstom's UK operations, with information from Poland, Tunisia, Hungary and Lithuania, and sought to rely on the evidence of the US conviction in the UK proceedings. This example highlights the danger that one authority will use information from another to launch an investigation of its own.

Authorities work together in a number of different ways. There are informal channels of communication, agreements or memoranda of understanding (MOU), formal information gateways and treaties for mutual legal assistance. Nevertheless, authorities may assist each other passively, such as by sharing information they have gathered during their investigations or obtaining publicly available records, or by taking a rather more active role, such as by interviewing

78 In response to requests under the Freedom Information Act 2000, the SFO published some limited information as to the volume of referrals it had received, from both domestic and overseas authorities, between 2012 and 2017. Notably, with regard to bribery and corruption referrals, the Foreign and Commonwealth Office was the SFO's greatest source of referrals (https://www.sfo.gov.uk/publications/corporate-information/freedom-of-information).

79 DOJ press release: 'Telia Company AB and Its Uzbek Subsidiary Enter Into a Global Foreign Bribery Resolution of More Than $965 Million for Corrupt Payments in Uzbekistan', dated 21 September 2017 (https://www.justice.gov/opa/pr/telia-company-ab-and-its-uzbek-subsidiary-enter-global-foreign-bribery-resolution-more-965).

80 DOJ press release: 'Alstom Pleads Guilty and Agrees to Pay $772 Million Criminal Penalty to Resolve Foreign Bribery Charges', dated 22 December 2014 (https://www.fbi.gov/news/pressrel/press-releases/alstom-pleads-guilty-and-agrees-to-pay-772-million-criminal-penalty-to-resolve-foreign-bribery-charges).

witnesses, providing logistical support to enable foreign authorities to conduct their own witness interviews and allowing secondments.[81]

Authorities share information, increasingly frequently and informally, on an 'intelligence only' basis. This has the advantage of speedily progressing an investigation by the exchange of, for example, banking, trading or company data without the delay associated with formal information channels. If the information is ultimately required for evidence in a criminal case, a formal route (i.e., a letter of request (LOR)) will be used to obtain the same information in evidential form.

9.8.2 Memoranda of understanding

Authorities commonly enter into MOU with authorities in their own or other jurisdictions where both exercise similar functions, or are concerned with the same issues (e.g., the PRA and the FCA have entered into a number of MOU with equivalent authorities in other jurisdictions[82]). Some multi-party MOU exist, such as the International Organization of Securities Commissions' Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information, to which over 109 parties are presently signatories.[83] MOU are not legally binding, but declare a shared commitment and aim to provide useful guidelines enabling faster and more efficient sharing of information.

Confidentiality clauses feature in MOU and there are carve-outs where to provide the information requested would violate domestic law or interfere with ongoing domestic criminal proceedings, for example.

9.8.3 Information gateways

There exist a number of statutory powers available to investigatory, regulatory and prosecution bodies to supply and share information with each other, domestically and internationally. These are commonly known as 'information gateways' and have a statutory basis.[84]

---

81 For example, in December 2016 the US DOJ Criminal Division announced it would second a lawyer to the UK for two years to work at the Financial Conduct Authority and the Serious Fraud Office, to further cooperation between the jurisdictions and share best practice. https://www.sfo.gov.uk/2016/12/09/us-department-justice-secondee/.

82 See, for example, the MOU between the Dubai Financial Services Authority and the PRA dated 12 June 2014 and the MOU between the Bank of Korea and the PRA & Bank of England dated 16 December 2014. Other examples include the MOU between the CFTC and FSA dated 17 November 2006 ('developed . . . in order to enhance their respective capabilities to address potential abusive or manipulative trading practices that may involve trading on UK and US derivatives exchanges') and the MOU between the SEC and the FCA dated 22 July 2013 concerning the consultation, co-operation and exchange of information related to the supervision of the relevant entities in the asset management industry.

83 May 2002, revised May 2012. A list of current signatories can be found here: http://www.iosco.org/about/?subSection=mmou&subSection1=signatories.

84 For instance, the information gateway for the SFO is in section 3(5) of the Criminal Justice Act 1987, for the CMA in Part 9 of the Enterprise Act 2002 (EA02) and the FCA and the PRA within section 349 of FSMA 2000.

For example, Part 9 of Enterprise Act 2002 prohibits the disclosure of information received by the CMA except, for example, where it is disclosing that information to another authority for the purpose of criminal proceedings. This gateway could be used in a LIBOR or FX-type investigation involving both criminal and competition issues.

There are limitations on the transmission of information. Any information so disclosed must be used only for the relevant purpose and the CMA must not make the disclosure unless it is satisfied that it is proportionate.[85] The CMA also must (so far as practicable) exclude from disclosure any information that is contrary to the public interest, commercial information that it believes might significantly harm the legitimate business interests of the undertaking to which it relates, or information relating to the private affairs of an individual, disclosure of which might significantly harm the individual's interests. Where the information is being transferred overseas additional limitations apply (e.g., seriousness of offence, appropriate local protection for the privilege against self-incrimination in criminal proceedings, storage of personal data).

Mutual legal assistance 9.8.4

Mutual legal assistance (MLA) is a formal method of co-operation between countries for obtaining assistance in the investigation or prosecution of criminal offences.[86] The nature of the assistance varies, but includes obtaining documentary evidence, conducting interviews, taking witness statements, requesting the execution of search warrants, freezing assets and producing bank documents.[87] Authorities will resort to MLA with their counterparties to receive evidence that cannot be gained through informal (and far quicker) means of co-operation, or where formal evidence is required. For instance, while one authority may ask another to obtain a witness statement, that authority will only be able to comply if the witness voluntarily agrees to give a statement. If that consent is not forthcoming, the requesting authority must instead resort to making an MLA request to compel the witness to provide evidence.

See Chapter 28 on extraterritoriality

An important limitation for requests under legal assistance treaties is that the requesting country must comply not only with its own laws but with the requested country's laws: meaning that in practice, MLA requests can be resource-intensive to prepare and serve.[88] However, in the United Kingdom, Unaoil's application for

85 Ibid.

86 In March 2017, the SFO published a response to a request made pursuant to the Freedom of Information Act listing the number of new and supplemental MLA requests it had executed on an annual basis between 2012 and 2017 (https://www.sfo.gov.uk/publications/corporate-information/freedom-of-information/). In 2016/17, the SFO accepted for execution 20 new MLA requests and 13 supplemental requests (down from 24 and 20 respectively in 2015/16).

87 Further guidance as to the types of assistance available from the UK authorities can be found in section 3 of the Home Office publication 'Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities Outside of the United Kingdom – 2015' (12th edition – May 2015).

88 In recent years, steps have been taken to simplify the legal framework for co-operation between Member States of the European Union on criminal investigations. European investigation orders

judicial review shows that there is a high bar for successfully challenging MLA requests through this mechanism.[89] Unaoil unsuccessfully applied to challenge the SFO's MLA request to the Monaco authorities for assistance in carrying out dawn raids, interviews and seizure of materials in Monaco, arguing that the letter requesting assistance failed to disclose key information about the case. The court made clear that the duty of candour, which attaches to UK search warrants, did not apply to MLA requests and that questions around the fairness of the raids and seizures should be resolved in accordance with local law. A successful judicial review challenge therefore would likely have to show that the SFO had no reasonable grounds for suspicion at the time the MLA request was made or that there was some other breach of the Crime (International Co-operation) Act, which gives the authority the power to request assistance from international authorities.

Voluntary co-operation with an authority can result in requests for the corporate to obtain documents from overseas where it can, as a demonstration of its ongoing and genuine co-operation.[90]

9.9 Strategies for dealing with multiple authorities

Companies should proceed on the assumption that authorities share or will share information and materials. It may be clear from the outset that an issue affecting a corporate operating in multiple jurisdictions would likely attract the attention of authorities in those countries. Alternatively, an authority may effectively be tipped off following a MLA request for assistance from a foreign authority and, on the basis of information provided pursuant to that request, commence its own investigation.

Accordingly, a coherent strategy for dealing with such attention should be formulated from the outset. The company may find it sensible to engage in an open and pragmatic dialogue with each authority regarding matters such as timetables and document requests, and be proactive in encouraging the authorities to take the same approach with each other wherever possible. Ultimately, if more than one agency has a legitimate basis on which to enforce, it is usually preferable to bring the matter to a combined resolution.

(EIOs) are judicial decisions taken in one Member State that are carried out by authorities in another. They relate to specific investigative measures to gather evidence in one Member State on behalf of another and allow for the sharing of evidence between Member States. EIOs were introduced into EU law through the EIO Directive 2014/41/EU and came into force in the United Kingdom on 31 July 2017 through the Criminal Justice (European Investigation Order) Regulations 2017, SI 2017/730.

89 *Unaenergy Group Holding Pte Ltd & Ors. v. The Director of the Serious Fraud Office* [2017] EWHC 600 (Admin).

90 Where a company does not voluntarily provide such documents, the SFO may seek to compel production. The English High Court ruled in the case of *R (KBR Inc.) v The SFO* [2018] EWHC 2012 (Admin) that the scope of the SFO's power to compel the production of data extends to: data of a UK company held abroad; and data of a non-UK company held abroad, provided there is a 'sufficient connection' between that company and the United Kingdom.

The following additional points should be considered when dealing with multi-agency investigations:

- Consider what enquiries or internal investigation should be conducted. An internal investigation will enable a company to quantify potential risk and to develop a strategy to cope with concurrent investigations. It can, however, be difficult to structure an internal investigation so that material generated is privileged in each jurisdiction involved (if privilege is even recognised). Moreover, potential exposures in one jurisdiction might mean enquiries elsewhere need to be more circumspect.
- Ensure that an appropriate employee (most likely a member of the in-house legal team) is given specific responsibility for co-ordinating the corporate's response to the investigations. Where international authorities are involved, the corporate should consider whether to form an internal response team to include employees from all affected jurisdictions.
- When formulating a strategy for dealing with concurrent investigations, consider which authorities are likely to be more influential or proactive and consider adopting an approach that takes into account their likely priorities or concerns.
- Engage specialised legal counsel to interface with law enforcement, including, where subject to overseas investigations, instructing and seeking advice from local counsel as necessary. This is particularly important if complying with a request for information from one authority may leave employees at risk of breaching data protection laws in other jurisdictions.
- Make sure that consistent explanations and documents are given (including considering whether developing a narrative 'script' may be helpful) and, so far as possible, that consistent approaches are adopted across all investigations (including coordination with local counsel and any other relevant external advisers).
- Where relevant, attempt to adopt a standardised approach to privilege across all investigations (which may necessitate careful negotiation with all authorities if approaches to privilege in their jurisdictions differ considerably).
- When considering whether to enter into settlement discussions, consider whether it would be beneficial to engage with all authorities at the same time. This may not be possible in circumstances where authorities are at differing stages in their investigation timetables, but would have the benefit of managing negative impacts such as business interruption, and harm to reputation and share price, as well as removing the need for ongoing company resources to be dedicated to overseeing the concurrent investigations. Encourage a holistic approach to sanctions across multiple jurisdictions, so as to avoid multiple monitorships or duplicative reparation and, where possible, to minimise fines.

Conclusion 9.10

Corporates are increasingly expected to co-operate with regulatory agencies and criminal authorities, even when such co-operation is voluntary. The DPAs corporates have entered into with the SFO demonstrate this expectation.

Corporates are coming under pressure from the public, stakeholders and government to act as good corporate citizens. Maintaining credibility with capital markets can be an additional factor in a decision to co-operate.

Co-operation is relevant at every stage of an investigation, and for every outcome. It requires continual and genuine assistance, prompt reporting of wrongdoing, and access to hard copy materials, electronic data and potential witnesses.

The conduct of internal investigations, witness interviews and legal privilege are becoming fraught battlegrounds.

Corporates should expect the involvement of multiple agencies across multiple jurisdictions as the co-operation between agencies and authorities increases.

10

Co-operating with the Authorities: The US Perspective

John D Buretta, Megan Y Lew and Courtney A Gans[1]

Government investigations of corporations can start quietly or loudly. A subpoena might arrive in the mail; an employee might speak up to a manager; federal agents might raid the offices and seize files, computers and cell phones; or border patrol agents might stop an employee, or a CEO, at the airport. However an investigation commences, a critical question at the outset is whether the company should co-operate in a government inquiry, and, if so, how, and to what extent. Like a game of chess, a company's opening moves can dictate the end game and must be chosen with care. In the best case, investigations quickly and cost-effectively point the authorities toward individual wrongdoers, the company's effort is short-lived, and it incurs no penalty. In the worst case, Pandora's box is opened.

While the decision to co-operate will turn on the unique factual and legal circumstances faced by a company, this chapter aims to guide the reader through the decision-making process, whether the investigation concerns the Foreign Corrupt Practices Act (FCPA), securities, antitrust or sanctions laws, or the False Claims Act, or other government actions. This chapter discusses how US government authorities define co-operation, identifies the pros and cons of co-operating with the authorities and discusses special considerations in multi-agency and cross-border investigations.

What is co-operation? 10.1

Co-operating with a US government authority generally entails providing all relevant, non-privileged information. This can amount to ensuring that key witnesses are available for interviews by the government, sharing information gleaned from

1 John D Buretta is a partner, Megan Y Lew is a practice area attorney and Courtney A Gans is an associate at Cravath, Swaine & Moore LLP.

internal interviews of employees, providing relevant documents as well as context and background for those documents, giving factual presentations, and agreeing to take remedial action where appropriate.

10.1.1 Department of Justice's general approach to co-operation

The Department of Justice (DOJ) issues guidance and policies for prosecutors in its Justice Manual. Its chapter on Principles of Federal Prosecution of Business Organizations sets forth ten factors that prosecutors should consider when investigating, deciding whether to charge and negotiating a plea or other agreement with a company. Among these is consideration for 'the corporation's willingness to cooperate, including as to potential wrongdoing by its agents'.[2] The Justice Manual states that a company is eligible for co-operation credit if it:

> *identif[ies] all individuals substantially involved in or responsible for the misconduct at issue, regardless of their position, status or seniority, and provide[s] to the Department all relevant facts relating to that misconduct. If a company seeking co-operation credit declines to learn of such facts or to provide the Department with complete factual information about the individuals substantially involved in or responsible for the misconduct, its co-operation will not be considered a mitigating factor under this section.*[3]

In other words, to obtain co-operation credit, a company must provide all non-privileged facts concerning misconduct.[4] In addition, the company must not intentionally remain ignorant about misconduct and cannot cherry-pick facts to share with the DOJ.

The DOJ's current approach to co-operation, as reflected in the Justice Manual, emphasises holding individuals accountable for their misconduct and strongly encourages companies to disclose the identities of individuals involved. Prior to September 2015, companies might obtain partial co-operation credit without identifying the individual wrongdoers to the DOJ; this might even have been sufficient to avoid charges in some instances.[5] In September 2015, the DOJ

2 US Dep't of Justice, Justice Manual § 9-28.300. Additional noteworthy factors include 'the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision' and 'the corporation's remedial actions, including, but not limited to, any efforts to implement an adequate and effective corporate compliance program or to improve an existing one, to replace responsible management, to discipline or terminate wrongdoers, or to pay restitution'. Id. In April 2019, the DOJ released a guidance document concerning these factors, entitled Evaluation of Corporate Compliance Programs, available at https://www.justice.gov/criminal-fraud/page/file/937501/download.

3 US Dep't of Justice, Justice Manual §§ 9-28.300, 9-28.700.

4 Id. § 9-28.720.

5 Sally Quillian Yates, Deputy Att'y Gen., US Dep't of Justice, Remarks at New York University School of Law Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing (10 September 2015), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

announced that co-operation would require disclosure of individual misconduct, regardless of the individual's title or seniority at the company.[6] The DOJ's newly announced approach in part reflected the inherent challenges in charging individuals in complex, white-collar investigations, where prosecutors often must sort through and understand 'complex corporate hierarchies, enormous volumes of electronic documents and a variety of legal and practical challenges that can limit access to the evidence' that the DOJ needs to bring charges against individuals, especially when evidence is located outside the United States.[7]

What does this mean in practice for a company under investigation? The DOJ wants to learn information such as: how and when the alleged misconduct occurred; who promoted or approved it; who was responsible for committing it;[8] and which individuals played significant roles in setting a company on a course of criminal conduct.[9] To provide this, company counsel may relay facts to the DOJ by producing relevant documents, allowing the DOJ to interview employees (including acquiescing to 'deconfliction' requests from the DOJ that the government interview employees before company counsel does so), proffering information obtained from an internal investigation or analysing voluminous or complex documents. To obtain full credit, the DOJ will consider the timeliness of the disclosures, whether the company undertook a proactive approach to co-operating, and the thoroughness of the company's investigation.[10] The DOJ does not expect companies to undertake a 'years-long, multimillion dollar investigation every time a company learns of misconduct'; rather, companies are expected 'to carry out a thorough investigation tailored to the scope of the wrongdoing'.[11] Nor does the DOJ want companies to delay their investigations 'merely to collect information about individuals whose involvement was not substantial, and who are not likely to be prosecuted'. The investigation should instead focus on individuals who had 'significant roles' in the misconduct.[12] In practice, companies seeking co-operation therefore need not 'have all the facts lined up on the first day' they

6 Id.

7 Id.

8 US Dep't of Justice, Justice Manual § 9-28.720.

9 Rod J. Rosenstein, Deputy Att'y Gen., US Dep't of Justice, Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

10 US Dep't of Justice, Justice Manual § 9-28.700.

11 Sally Quillian Yates, Deputy Att'y Gen., US Dep't of Justice, Remarks at the New York City Bar Association White Collar Crime Conference (10 May 2016), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-q-yates-delivers-remarks-new-york-city-bar-association.

12 Rod J. Rosenstein, Deputy Att'y Gen., US Dep't of Justice, Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

talk to the DOJ, but they should turn over relevant information to the DOJ on a rolling basis as they receive it.[13]

To ensure that the company's disclosures to the DOJ are extensive and that its internal investigation is thorough, and to fulfil the DOJ's own obligation to make just decisions based on the fullest possible set of facts, the DOJ usually undertakes its own parallel investigation. Accordingly, the Justice Manual instructs prosecutors to:

> *proactively investigat[e] individuals at every step of the process – before, during, and after any corporate co-operation. Department attorneys should vigorously review any information provided by companies and compare it to the results of their own investigation, in order to best ensure that the information provided is indeed complete and does not seek to minimize, exaggerate, or otherwise misrepresent the behaviour or role of any individual or group of individuals.*[14]

Counsel may encounter situations where it is unclear whether misconduct has actually occurred, either because the corporate client does not have access to the relevant information or, even with full access, cannot discern whether there is malfeasance. In this regard, the DOJ has emphasised that it 'just want[s] the facts' – it does not expect counsel for the company 'to make a legal conclusion about whether an employee is culpable, civilly or criminally'.[15]

In other cases, a company may find that relevant documents in a foreign location cannot be produced to US authorities because of foreign data privacy, bank secrecy or other blocking laws. The Justice Manual recognises that such situations may occur and acknowledges that a company may still be eligible for co-operation credit, though the company will bear the burden of explaining why co-operation credit is still justified despite the restrictions faced by the company in gathering or disclosing certain facts.[16]

The DOJ has emphasised that co-operation does not require a company to waive the attorney–client privilege or the attorney work-product protection.[17] While a company may decide to waive these privileges and protections when it suits its interests to do so, prosecutors may not request such a waiver.[18]

13 Sally Quillian Yates, Deputy Att'y Gen., US Dep't of Justice, Remarks at the New York City Bar Association White Collar Crime Conference (10 May 2016), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-q-yates-delivers-remarks-new-york-city-bar-association.

14 US Dep't of Justice, Justice Manual § 9-28.700.

15 Id.

16 Id.

17 US Dep't of Justice, Justice Manual § 9-28.710.

18 Id. See also Memorandum from Mark Filip, Deputy Attorney Gen., US Dep't of Justice, to Heads of Department Components and United States Attorneys (28 August 2008), available at https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf.

Other Department of Justice policies regarding co-operation 10.1.2

Several components of the DOJ maintain policies regarding company co-operation separate from the guidelines set out in the Justice Manual. Three examples are discussed below: (1) the Criminal Division's policy regarding FCPA enforcement, (2) the Antitrust Division's leniency programme and (3) the Civil Division's False Claims Act enforcement policy.

The FCPA Pilot Program and Corporate Enforcement Policy 10.1.2.1

In April 2016, the DOJ announced a pilot programme for FCPA cases with the goal of motivating 'companies to voluntarily self-disclose FCPA-related misconduct, fully cooperate with the [DOJ Criminal Division's] Fraud Section, and, where appropriate, remediate flaws in their controls and compliance programs'.[19] The Pilot Program, which was initially meant to last one year, became a permanent DOJ programme in November 2017.[20] Known as the FCPA Corporate Enforcement Policy, it is designed to encourage companies to self-report any potential FCPA violations and promote increased co-operation with the DOJ.

To be eligible for the full benefits of the FCPA Corporate Enforcement Policy, companies must: (1) voluntarily self-report all facts within a reasonably prompt time, (2) offer full co-operation, and (3) undertake remedial measures in a timely fashion. In addition, the company must disgorge itself of all profits related to the misconduct. In exchange, the company is eligible to receive up to a 50 per cent reduction in any applicable fines and may avoid the necessity of appointing a monitor.[21] If a company complies with these three requirements, the DOJ will apply a presumption that the matter will be resolved through a declination.[22] 'That presumption may be overcome only if there are aggravating circumstances related to the nature and seriousness of the offense, or if the offender is a criminal recidivist.'[23] If aggravating circumstances lead the DOJ to determine that declination is not appropriate, the DOJ will nonetheless recommend a 50 per cent reduction off the low end of the US Sentencing Guidelines' fine range appropriate to the offence.[24] To date, the DOJ has issued over a dozen declination letters under the FCPA Corporate Enforcement Policy.[25]

In November 2019, the DOJ made clarifying revisions to certain provisions of the FCPA Corporate Enforcement Policy. First, the DOJ changed a policy that stated a company must alert theDOJ when it 'is or should be aware of

19 Leslie R Caldwell, Ass't Attorney General (5 April 2016), available at https://www.justice.gov/archives/opa/blog/criminal-division-launches-new-fcpa-pilot-program.

20 Rod Rosenstein, Deputy Attorney General, Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (29 November 2017), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-34th-international-conference-foreign.

21 Id.

22 Id.

23 Id.

24 Id.

25 US Dep't of Justice, Declinations (26 September 2019), available at https://www.justice.gov/criminal-fraud/corporate-enforcement-policy/declinations.

opportunities' to 'obtain relevant evidence not in the company's possession and not otherwise known to the Department'. The change removed the wording 'should be' and replaced it with 'is aware', so that the company must now only report opportunities to obtain evidence not in its possession when it is actually aware of such evidence. Second, the November update makes clear that self-disclosure following only a preliminary investigation is acceptable and may earn self-disclosure credit. A footnote in the self-disclosure section now underscores that a company 'may not be in a position to know all relevant facts at the time of a voluntary self-disclosure, especially where only preliminary investigative efforts have been possible' and provides that companies should make clear during a self-disclosure when their knowledge is based on a preliminary investigation. Third, the DOJ clarified that to receive self-disclosure credit, companies must turn over all relevant facts related to 'any individuals' who played a substantial part in the 'misconduct at issue'. The previous version of the policy stated that companies must turn over relevant facts related to 'all individuals' who played a part in a 'violation of law'. This new terminology makes it clear that a company need not determine that there has been a violation early on in the investigation in order to turn over information necessary for self-disclosure credit.[26]

10.1.2.2 The antitrust leniency programme

The DOJ Antitrust Division has a corporate leniency programme granting leniency to the first company that (1) self-discloses conduct related to unlawful anti-competitive conspiracies and (2) co-operates with the DOJ's ensuing investigation.[27] A company that has been granted leniency is only liable for the actual damages in related follow-on litigation, rather than treble damages. Additionally, a company given leniency is not liable for the damages caused by other members of the conspiracy, which a conspirator typically would be responsible for under a theory of joint-and-several liability in antitrust conspiracy cases.

10.1.2.3 The False Claims Act

In May 2019, for the first time, the DOJ issued guidelines for awarding entities with co-operation credit in False Claims Act (FCA) cases. The FCA, frequently used in healthcare litigation, imposes civil liability on entities that defraud government programmes. While the new federal guidance does not present any radically new considerations, it does provide helpful standards and brings FCA cases in line with existing DOJ practices in other types of investigations.[28]

---

26 Judy Godoy, 'DOJ Tweaks FCPA Corporate Enforcement Policy for Clarity', Law360 (20 November 2019) available at https://www.law360.com/securities/articles/1221939/doj-tweaks-fcpa-corporate-enforcement-policy-for-clarity; FCPA Corporate Enforcement Policy at 9-47.120.

27 Frequently Asked Questions About the Antitrust Division's Leniency Program and Model Leniency Letters (26 January 2017), available at https://www.justice.gov/atr/page/file/926521/download.

28 Peter Hutt, Michael Wagner, Michael Maya and Brooke Stanley, 'New DOJ Cooperation Credit Guidelines a Welcome Sign, but Key Questions Remain Unresolved', available at

The federal guidance contemplates eligibility for co-operation credit in FCA matters in three circumstances. First, eligibility is available for voluntary self-disclosure by entities that discover conduct that violates the FCA. Notably, co-operation credit is not limited to entities that self-disclose before an investigation commences. Rather, if '[d]uring the course of an internal investigation into the government's concerns . . . entities . . . discover additional misconduct going beyond the scope of the known concerns, . . . the voluntary self-disclosure of such additional misconduct will qualify the entity for credit.'[29] Second, co-operation credit is available for entities providing assistance to an ongoing government investigation, including, but not limited to, identifying employees or individuals responsible for the misconduct, accepting responsibility for the misconduct, making employees available for depositions and interviews, and preserving and collecting relevant information and data in excess of what is required by law. Finally, entities that undertake remedial measures in response to an FCA violation may also be eligible for co-operation credit.

Approaches to co-operation by other federal agencies 10.1.3

Other US enforcement agencies take similar approaches to rewarding company co-operation. Two examples of such agency processes – the US Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) – are described below.

The SEC's approach to co-operation was first described in a report of investigation and statement regarding the public company Seaboard.[30] This report, which became known as the 'Seaboard Report', concluded that charges against Seaboard were not warranted based on the consideration of four broad factors: (1) self-policing by the company prior to the discovery of the misconduct; (2) self-reporting the misconduct to the SEC, including investigating the misconduct; (3) remediation of the misconduct; and (4) co-operation with the SEC.[31] The benefits of co-operating with the SEC could range from the SEC 'declining an enforcement action, to narrowing charges, limiting sanctions or including mitigating or similar language in charging documents'.[32] Entry into a deferred or non-prosecution agreement may also be an option depending on the level of

https://www.insidegovernmentcontracts.com/2019/05/new-doj-cooperation-credit-guidelines-a-welcome-sign-but-key-questions-remain-unresolved/.

29 US Dep't of Justice, Justice Manual § 4-4.112.

30 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Co-operation to Agency Enforcement Decisions, Release No. 34-44969 (23 Oct. 2001) (Seaboard Report), available at https://www.sec.gov/litigation/investreport/34-44969.htm.

31 Id. See also US Securities and Exchange Commission, Spotlight on Enforcement Cooperation Program (20 Sept. 2016), available at https://www.sec.gov/spotlight/enforcement-cooperation-initiative.shtml.

32 Andrew Ceresney, Director, SEC Division of Enforcement, Remarks at University of Texas School of Law's Government Enforcement Institute in Dallas, Texas (13 May 2015), available at https://www.sec.gov/news/speech/sec-co-operation-program.html.

co-operation from the company.[33] Similar to the DOJ's current approach, the SEC expects a co-operating company to provide 'the Commission staff with all information relevant to the underlying violations and the company's remedial efforts'.[34]

The CFTC, which regulates US derivatives markets, also offers co-operation credit. While the CFTC has had a longstanding policy of offering co-operation credit, in 2017 it issued advisories that further incentivised 'individuals and companies to cooperate fully and truthfully in CFTC investigations and enforcement actions'.[35] Similar to the approaches adopted by the DOJ and SEC, the CFTC will, in its discretion, consider the following broad factors in determining whether to grant co-operation credit: (1) 'the value of the co-operation' to the instant investigation and enforcement action; (2) 'the value of the co-operation to the [CFTC's] broader law enforcement interests'; (3) 'the culpability of the company or individual and other relevant factors'; and (4) 'uncooperative conduct that offsets or limits credit that the company or individual would otherwise receive'.[36] The CFTC's advisories emphasise that co-operation credit will be given to co-operation that is 'sincere', 'robust' and 'indicative of a willingness to accept responsibility for the misconduct'.[37] The benefits of co-operating with the CFTC range from the agency taking no enforcement action to imposing reduced charges against the co-operating company.[38] Furthermore, in March 2019, the CFTC announced a new advisory on self-reporting and co-operation to build on the existing foundation of co-operation to further incentivise 'individuals and

33 Id. See, e.g., Deferred Prosecution Agreement between Tenaris, S.A. and the SEC (23 March 2011), available at https://www.sec.gov/news/press/2011/2011-112-dpa.pdf; Non-Prosecution Agreement between Akami Technologies, Inc. and the SEC (3 May 2016), available at https://www.sec.gov/news/press/2016/2016-109-npa-akamai.pdf.

34 US Securities and Exchange Commission, Spotlight on Enforcement Cooperation Program (20 September 2016), available at https://www.sec.gov/spotlight/enforcement-cooperation-initiative.shtml.

35 US Commodity Futures Trading Commission, Release Number 7518-17, CFTC's Enforcement Division Issues New Advisories on Co-operation (19 January 2017), available at https://www.cftc.gov/PressRoom/PressReleases/pr7518-17. See US Commodity Futures Trading Commission, Enforcement Advisory: Co-operation Factors in Enforcement Division Sanction Recommendations for Companies (19 January 2017), available at https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisorycompanies011917.pdf; US Commodity Futures Trading Commission, Enforcement Advisory: Co-operation Factors in Enforcement Division Sanction Recommendations for Individuals (19 January 2017), available at https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisoryindividuals011917.pdf.

36 US Commodity Futures Trading Commission, Release Number 7518-17, CFTC's Enforcement Division Issues New Advisories on Co-operation (19 January 2017), available at https://www.cftc.gov/PressRoom/PressReleases/pr7518-17.

37 US Commodity Futures Trading Commission, Enforcement Advisory: Co-operation Factors in Enforcement Division Sanction Recommendations for Companies (19 January 2017), available at https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisorycompanies011917.pdf.

38 Id.

companies to self-report misconduct, cooperate fully in CFTC investigations and enforcement actions, and appropriately remediate to ensure the wrongdoing does not happen again'.[39]

The CFTC advisories collectively list dozens of specific and concrete factors that the agency will consider when assessing whether to grant co-operation credit.[40] Company counsel may find it beneficial to refer to these factors when determining the company's course of action at various points in time, such as when learning about misconduct, investigating misconduct, self-disclosing misconduct to government authorities and co-operating with government authorities. For example, the advisory concerning co-operation by companies includes a section concerning the 'quality' of the company's co-operation, which the advisory states should be assessed by looking at whether the company 'willingly used all available means to . . . preserve all relevant information', 'make employee testimony' or company documents 'available in a timely manner', 'explain transactions and interpret key information', and 'respond quickly to requests and subpoenas for information from the CFTC', among other things.[41] Indeed, these considerations are relevant to any situation where a company is considering co-operating with authorities, regardless of the type of misconduct or whether the misconduct falls under the jurisdiction of the CFTC.

Case study: Walmart 10.1.4

Choosing to co-operate with the government is not a one-size-fits-all decision, and companies often may choose to (or be able to) co-operate with some aspects of a government investigation, but not others. For example, in June 2019, Walmart Inc and a Brazilian Walmart subsidiary agreed to pay US$137 million to settle criminal charges brought by the DOJ in connection to alleged FCPA violations. These allegations arose out of conduct that occurred from 2000 to 2011, in which Walmart employees failed to implement and maintain the company's internal accounting controls to prevent improper payments to foreign government officials. This lapse in controls allowed Walmart subsidiaries in Mexico, India, Brazil and China to hire third-party intermediaries who, in turn, made improper gifts and payments to foreign officials to open store locations in those countries without delay, avoiding detection from Walmart's accounting system. Crucially, certain senior executives at the company were aware of this lapse in controls, yet these practices persisted.[42]

39 US Commodity Futures Trading Commission, CFTC Division of Enforcement Issues Advisory on Violations of the Commodity Exchange Act Involving Foreign Corrupt Practices, Release No. 7884-19 (9 March 2019), available at https://www.cftc.gov/PressRoom/PressReleases/7884-19.

40 See US Commodity Futures Trading Commission, Enforcement Advisory: Co-operation Factors in Enforcement Division Sanction Recommendations for Companies (19 January 2017), available at https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisorycompanies011917.pdf.

41 Id.

42 US Dep't of Justice, 'Walmart Inc. and Brazil-Based Subsidiary Agree to Pay $137 Million to Resolve Foreign Corrupt Practices Act Case', press release (20 June 2019), available at

Walmart's co-operation with the government led to a reduction in the overall fine that was levied against the company. Walmart fully co-operated with the investigations into conduct in Brazil, China and India; however, it did not provide full documents and information in connection with the Mexican investigation and chose to interview a key witness before making the witness available for a DOJ interview, contrary to the DOJ's request. Furthermore, Walmart did not self-disclose the misconduct that occurred in Mexico, while it had disclosed the conduct in the other countries. Because Walmart fully co-operated with the investigations in Brazil, China and India, it received a 25 per cent reduction in the fines applicable to those jurisdictions under the US Sentencing Guidelines, while it only received a 20 per cent reduction in the fines applicable to the Mexican misconduct.[43]

10.2 Key benefits and drawbacks to co-operation

Deciding whether to co-operate with a government investigation requires careful consideration of the associated benefits and drawbacks. On the one hand, co-operation affords the opportunity of reduced or no charges and penalties; however, co-operation also brings other risks.

10.2.1 Reduced or no charges and penalties

By and large, companies and individuals choose to co-operate with the government to receive some leniency in the form of reduced (or even no) penalties or charges. Research has shown that companies that choose to co-operate with the government tend to achieve better outcomes and typically end up paying lower fines than those that do not.[44] For example, in 2016, Dutch telecommunications company VimpelCom (now known as VEON) paid a criminal fine to the DOJ and Dutch authorities of US$460 million rather than US$836 million to US$1.67 billion, as suggested by the US Sentencing Guidelines, because of the Dutch telecommunications company's co-operation with the DOJ in its investigation of alleged FCPA violations.[45] On the other hand, in 2015, Alstom SA was required to pay a criminal fine of US$772 million, the largest-ever recorded fine for FCPA violations at that time, in part because of 'Alstom's failure to voluntarily

https://www.justice.gov/opa/pr/walmart-inc-and-brazil-based-subsidiary-agree-pay-137-million-resolve-foreign-corrupt.

43 Id.

44 See, e.g., Alan Crawford, 'Research Shows It Pays To Cooperate With Financial Investigations, Impact' (June 2014), available at http://pac.org/wp-content/uploads/Impact_06_2014.pdf.

45 US Dep't of Justice, 'VimpelCom Limited and Unitel LLC Enter into Global Foreign Bribery Resolution of More Than $795 Million; United States Seeks $850 Million Forfeiture in Corrupt Proceeds of Bribery Scheme', press release (18 February 2016), available at https://www.justice.gov/opa/pr/vimpelcom-limited-and-unitel-llc-enter-global-foreign-bribery-resolution-more-795-million.

disclose the misconduct . . . [and] Alstom's refusal to fully cooperate with the department's investigation for several years'.[46]

In addition to the reduced monetary fines that can result from co-operation, the form of a penalty may also vary depending on whether, and how much, a company co-operates with government authorities. If a company has fully co-operated, the government may consider offering a declination (the government declines to prosecute the entity for any alleged wrongdoing), if the facts and circumstances warrant such a resolution. If a declination is not an option, the next best scenario is a non-prosecution agreement (NPA), which is a contractual agreement between the wrongdoer and the government in which the government agrees not to bring criminal charges in exchange for certain requirements from the company (e.g., a fine, admitting to certain facts, further co-operating with the government or entering into compliance or remediation efforts). Another option in the government's toolbox is a deferred prosecution agreement (DPA), which is an agreement with the government where criminal charges are filed with the court but prosecution is postponed for a certain period in exchange for the company undertaking certain conditions (e.g., payment of fines, compliance reforms, further co-operating with the government, annual reporting or certification requirements, or the appointment of a monitor). If the company complies with these conditions, the government will move to dismiss the charges at the end of the term of deferment. Unlike NPAs, DPAs require court approval, which is usually granted. Finally, if the government believes a stronger penalty is warranted, it could request that a subsidiary of the company, rather than the parent, enter a guilty plea, which can reduce some of the collateral consequences facing the parent company had it been required to plead guilty.

Suspension and debarment 10.2.2

In addition to criminal fines, companies may also face collateral damage from pleading guilty, or otherwise admitting to wrongdoing. For instance, companies in the healthcare, defence and construction fields are particularly vulnerable because any admissions of wrongdoing could have the collateral consequence of excluding them from eligibility for the government contracts on which their business heavily relies. Furthermore, any admission of wrongdoing could trigger a host of civil litigation from shareholders or other claimants. Similarly in the Employee Retirement Income Security Act (ERISA) sphere, entities that have registered as a qualified professional asset manager, allowing them to work with pension funds and make investments for ERISA clients, may have their status revoked by the Department of Labor if key individuals or the company has been convicted of a crime. Likewise, for companies regulated by the SEC, enforcement actions can result in suspension, disbarment, or both, from the securities markets. Furthermore, even if an issuer is not disqualified altogether, it can lose

46 US Dep't of Justice, 'Alstom Sentenced to Pay $772 Million Criminal Fine to Resolve Foreign Bribery Charges', press release (13 November 2015), available at https://www.justice.gov/opa/pr/alstom-pleads-guilty-and-agrees-pay-772-million-criminal-penalty-resolve-foreign-bribery.

its well-known seasoned issuer status if it has been found to violate the securities laws. This can have a significant impact on an issuer's ability to quickly file registration statements with the SEC and the issuer's ability to appropriately time the market when offering securities for sale.[47]

See Chapter 26 on fines, disgorgement, etc

In July 2019, the SEC announced that it was changing certain rules related to settlement offers to streamline the process for issuers seeking to settle violations of the securities laws and, concurrently, requesting a waiver from certain collateral consequences of such violations. Chairman Jay Clayton announced:

> *Recognizing that a segregated process for considering contemporaneous settlement offers and waiver requests may not produce the best outcome for investors in all circumstances, I believe it is appropriate to make it clear that a settling entity can request that the [SEC] consider an offer of settlement that simultaneously addresses both the underlying enforcement action and any related collateral disqualifications.*[48]

The simultaneous review of offers of settlement and requests for waivers is a noteworthy development because previously the SEC considered these requests separately, resulting in longer delay and uncertainty for issuers it regulates.[49]

10.2.3 Financial cost

While co-operation between company counsel and the DOJ can save scarce government resources, it often represents a significant cost for the company itself. A company may generally be better placed to run an investigation because conceivably it may know where information is housed and whom to talk to, and can more readily determine the relevant facts and documents at issue. Running a high-quality, diligent and thorough internal investigation, despite the relative ease of doing so, is expensive. Document review of company emails, hiring external counsel, travel to and from interviews and preparing presentations to the government, all add up to significant expense. Moreover, if individual employees are implicated in the wrongdoing, they may also choose to hire their own counsel who will also perform an investigation, albeit in a more limited fashion, for which the company may bear financial responsibility. Finally, companies that are found to have committed misconduct may also need to reimburse the victims of their

47 Adam Hakki et al., 'SEC Chairman Announces Significant Changes To Commission Procedures For Considering Disqualification Waivers', Shearman & Sterling (7 August 2019), available at https://www.shearman.com/perspectives/2019/08/sec-chairman-announces-significant-changes-to-commission-procedures.

48 Jay Clayton, Chairman US Securities and Exchange Commission, 'Statement Regarding Offers of Settlement', Public Statement, (3 July 2019), available at https://www.sec.gov/news/public-statement/clayton-statement-regarding-offers-settlement.

49 Adam Hakki et al, Sec Chairman Announces Significant Changes To Commission Procedures For Considering Disqualification Waivers, Shearman & Sterling (7 August2019), available at https://www.shearman.com/perspectives/2019/08/sec-chairman-announces-significant-changes-to-commission-procedures.

misconduct for certain expenses or pay restitution, which could be considerable and affect other aspects of an investigation or settlement. For example, in 2016, asset management firm Och-Ziff (now named Sculptor Capital Management) agreed to a US$213 million criminal settlement with the DOJ and SEC for violations of the FCPA. In September 2019, however, Judge Garaufis of the Eastern District of New York ruled that certain former investors in a Congolese mine should be classified as victims of Och-Ziff's misconduct, raising the question of whether those investors would be entitled to restitution from the firm. While Judge Garaufis has not yet ruled on whether, and in what amount, these investors are entitled to restitution, the investors claim that they are entitled to US$1.8 billion, opening up the possibility that Och-Ziff may be obligated to pay out more than it agreed to in its settlement with the government. Och-Ziff and the DOJ will submit further briefing on this issue.[50]

Recently, there has also been a trend of victims attempting to recoup the costs of their own internal investigations in connection to misconduct under principles of restitution. In May 2018, however, the United States Supreme Court held that the Mandatory Victims Restitution Act's (MVRA) provision for reimbursement of expenses related to investigations only applied to government investigations and not to private investigations undertaken by a victim.[51] The MVRA requires that certain convicted felons 'reimburse the victim for lost income and necessary child care, transportation, and other expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense'.[52] The Court found that the MVRA does not 'cover the costs of a private investigation that the victim chooses on its own to conduct, which are not "incurred during" participation in a government's investigation'.[53] Even if 'the victim shared the results of its private investigation with the Government', that does not mean that the private investigation was 'necessary' under the MVRA.[54]

Disruption to business 10.2.4

Any business executive or in-house counsel will know keenly that an investigation, regardless of whether the company chooses to co-operate with government authorities, will result in some amount of disruption to key business activities. While declining to co-operate with an investigation should not in and of itself indicate an organisation's culpability, it could have negative public relations consequences as investors and other third-party stakeholders may view this as indicative of guilt or the degree of financial penalty. The Justice Manual does make clear, however, that 'the decision not to co-operate by a corporation . . . is not itself

See Chapter 39 on protecting corporate reputation

50 Dylan Tokar, 'Restitution Battle Throws Three-Year-Old Och-Ziff Settlement Into Limbo', *Wall St. J.* (7 September 2019), available at https://www.wsj.com/articles/restitution-battle-throws-three-year-old-och-ziff-settlement-into-limbo-11567810832.

51 *Lagos v. United States*, 138 S. Ct. 1684, 1685-6 (2018).

52 18 U.S.C. § 3663A(b)(4).

53 *Lagos v. United States*, 138 S. Ct. 1684, 1686 (2018).

54 Id.

evidence of misconduct at least where the lack of co-operation does not involve criminal misconduct or demonstrate consciousness of guilt.'[55]

Whether or not a company chooses to co-operate with the government in an investigation, any investigation will cause disruption to the company's daily operations, and may even affect share prices. For example, an investigation can take up executives' time and attention; in-house counsel must coordinate extensively with external counsel; any key witnesses have to set aside time to be prepped and interviewed and financial resources may need to be diverted to help cover the costs of complying with or conducting an internal investigation.

Furthermore, investigations often bring about significant uncertainty for a business, depending on the seriousness and scale of the investigation. Investors may lose confidence in the company's financial prospects, especially because it may be necessary to divulge details related to the investigation to lenders and other third-party finance partners even before the investigation has been concluded (including details that have not been disclosed publicly). In the event that a company is facing the prospect of paying a substantial financial penalty in an investigation, lenders may choose to withdraw funding or revaluate the terms of any outstanding loans, causing the company's share price to drop accordingly.[56]

10.2.5 Exposure to civil litigation

Companies that co-operate with the government are often at risk of follow-on civil litigation based on any admissions or acceptance of lesser charges in connection with an investigation. Many investigations result in companies making certain admissions to the government, which potential plaintiffs can use to base any civil ligation on, either through class or derivative actions. These civil actions can also have significant financial ramifications. For example, civil penalties in the antitrust sphere can result in treble damages.[57] Because of the associated risks of derivative civil actions, companies may ultimately decide that the cost of co-operation is simply too high, and instead decide to decline to co-operate and deny liability and risk defending the company's innocence at trial.

A government investigation or admission of guilt may only be the first stage of a company's legal issues. For example, in 2014, following an investigation, the SEC charged Avon Products with having violated the FCPA for failing to put in place comprehensive controls for detecting instances of bribery in China. Avon settled the civil and criminal cases by agreeing to a fine of US$135 million. This resulted in shareholders filing several securities class action lawsuits against the company, claiming that Avon's management failed to put in place adequate controls to prevent FCPA violations, causing the company to lose millions of dollars of shareholder money through the cost of the related investigations and government fines. Ultimately, the case was dismissed because the court declined to find

55 US Dep't of Justice, Justice Manual § 9-28.700.

56 See, e.g., US Dep't of Justice, Justice Manual § 9-28.700 ('a protracted government investigation . . . could disrupt the corporation's business operations or even depress its stock price').

57 15 U.S.C. § 15(a).

that the FCPA created a private right of action; however, the resultant civil litigation cost yet more resources and time.[58]

VEON (formerly known as VimpelCom) faced similar ramifications following a government investigation in 2017. VEON's share prices dropped after it disclosed that it was under investigation by US and Dutch government authorities for potential FCPA violations and was conducting its own internal investigation. Ultimately, VEON entered into a DPA with the US government and paid roughly US$460 million in penalties. Additionally, the company had spent nearly US$900 million in related investigation and litigation costs. VEON shareholders brought a securities fraud action against the company, claiming that it had failed to disclose that the company's gains were the result of bribes paid to foreign governments in violation of the FCPA. The plaintiffs relied on certain admissions that VEON had made in connection with its deferred prosecution agreement, which the court ultimately decided were actionable.[59]

See Chapter 34 on parallel civil litigation

Excessive co-operation between counsel and the government 10.2.6

At what point is co-operation and coordination between the DOJ and company counsel too much? There have been a few instances where a company's internal investigation is deemed to be so entangled with a government investigation and government and company counsel are so coordinated, that it appears as if the government has 'outsourced' its investigatory authority. This can cause problems later down the line. For example, a company's investigation records could become subject to discovery, even if those records would otherwise be considered privileged. Additionally, a court could decide to exclude certain evidence or testimony for running afoul of certain constitutional provisions, even if that testimony was elicited by company counsel and not the government.

While judicial oversight of internal investigations is rare, recent developments suggest some judges may be more hostile to the perceived 'outsourcing' of criminal investigations to the private sector. In *United States v. Connolly*, Judge McMahon of the Southern District of New York issued a decision in May 2019 that was highly critical of the degree of coordination between the DOJ and Deutsche Bank's external counsel involving an internal investigation ostensibly run by the bank's external counsel.[60] The investigation involved allegations that several banks, including Deutsche Bank, unlawfully manipulated the setting of LIBOR interest rates.[61] Deutsche Bank launched an internal investigation into the misconduct and eventually entered into a DPA with the DOJ.[62]

58 Benjamin Galdston, 'Shareholder Litigation for Waste of Corporate Assets in Internal FCPA Investigations', The Review of Securities & Commodities Regulation (18 April 2018), available at https://s3.amazonaws.com/documents.lexology.com/9877aa80-bdfa-49fb-871b-734a74300baa.pdf.

59 Id.

60 No. 16 Cr. 0370 (CM) (ECF No. 432) (Opinion Denying Defendant Gavin Black's Motion for Kastigar Relief) (Connolly) (S.D.N.Y. 2 May 2019).

61 Id.

62 Id.

Two former Deutsche Bank traders, Matthew Connolly and Gavin Campbell Black, were subsequently indicted. During his trial, Black moved to suppress statements he had made in connection with Deutsche Bank's internal investigation, arguing that, because the DOJ had effectively 'outsourced' its own investigation function to Deutsche Bank's company counsel, his statements had actually been compelled by the US government in violation of his right against self-incrimination.[63] Because Black's statements were not used at trial, before the grand jury or during its investigation, Judge McMahon found that Black's rights against self-incrimination were not actually violated.[64] She did, however, write a scathing summation of the degree of coordination between the DOJ and Deutsche Bank's company counsel, writing that:

> *[R]ather than conduct its own investigation, the Government outsourced the important developmental stage of its investigation to Deutsche Bank – the original target of that investigation . . . Deutsche Bank . . . effectively deposed their employees by company counsel and then turned over the resulting questions and answers to the investigating agencies.*[65]

Since *Connolly* was decided recently, it is currently unclear how it will impact a company's internal investigations and ensuing co-operation with government authorities. Judge McMahon stopped short of saying that any level of coordination at all is impermissible. To steer clear of this risk, company counsel are advised to carefully evaluate (and re-evaluate) their relationship to the government and ensure that they are keenly aware of how their fiduciary duties may differ from and conflict with those of the government.

10.2.7 Other options besides co-operation

Co-operation is not the only option for companies or individuals when facing a government investigation. While companies that co-operate are generally guaranteed leniency, there are situations in which co-operation many not effectively prevent prosecution or reduce a financial penalty, which the Justice Manual guidelines themselves acknowledge: 'The government may charge even the most cooperative corporation . . . if . . . the prosecutor determines that a charge is required in the interests of justice. Put differently, even the most sincere and thorough effort to cooperate cannot necessarily absolve a corporation that has . . . engaged in an egregious, orchestrated, and widespread fraud.'[66] Therefore, there are situations when it is actually pointless to pursue co-operation and other methods must be employed.

First, the company can request a meeting with authorities to explain why the allegations do not amount to an actual violation of law or the particular agency

63 Id.
64 Id.
65 Id.
66 US Dep't of Justice, Justice Manual § 9-28.720.

does not have jurisdiction. Second, the defendant could challenge the jurisdiction of the court or regulator's jurisdiction to investigate the matter. Third, companies always have the option to fight the charges on the merits based on insufficiency of evidence in a court of law. This method was employed to dramatic effect by FedEx, when it refused to settle charges that it had conspired to ship illegal prescription drugs to online pharmacies. Just four days into the trial, the DOJ voluntarily dismissed the charges, stating that it had insufficient evidence to proceed.[67] Meanwhile, United Parcel Service, Google, Walgreens Company and CVS Caremark Corporation had to pay hefty fines after settling with the government.

Special challenges with multi-agency and cross-border investigations 10.3

Multi-agency coordination 10.3.1

Multi-agency coordination is a crucial element of successfully resolving any large, corporate investigation in which multiple US agencies are involved. In 2012, the DOJ issued guidance, which solidified long-standing agency practice, to ensure that 'Department prosecutors and civil attorneys coordinate together and with agency attorneys in a manner that adequately takes into account the government's criminal, civil, regulatory and administrative remedies'.[68] The policy statement emphasises 'that criminal prosecutors and civil trial counsel should timely communicate, coordinate, and cooperate with one another and agency attorneys to the fullest extent appropriate to the case and permissible by law' by ensuring that 'criminal, civil and agency attorneys coordinate in a timely fashion, discuss common issues that may impact each matter, and proceed in a manner that allows information to be shared to the fullest extent appropriate to the case and permissible by law'.[69] Furthermore, the Justice Manual has policies obliging departmental attorneys to consider the possibility of any parallel proceeding '[f]rom the moment of case intake' and discuss remedies and communication with other interested investigatory agents and to 'consider investigative strategies that maximize the government's ability to share information among' various agencies.[70] Additionally, the Justice Manual directs prosecutors to assess '[a]t every point between case intake and final resolution . . . the potential impact of [agency] actions on criminal, civil, regulatory and administrative proceedings'.[71]

In practice, each agency has its own processes and time frames for investigating alleged misconduct and approving settlements. As a result, on occasion, it can

67 Dan Levine, US Ends $1.6 billion Criminal Case Against FedEx (17 June 2016), available at https://www.reuters.com/article/us-fedex-pharmaceuticals-judgment-idUSKCN0Z32HC.

68 US Attorney General, 'Memorandum for all United States Attorneys Director, Federal Bureau of Investigation, All Assistant United States Attorneys, All Litigating Divisions, All Trial Attorneys', US Dep't of Justice, (30 January 2012), available at https://www.justice.gov/jm/organization-and-functions-manual-27-parallel-proceedings.

69 Id.

70 US Dep't of Justice, Justice Manual § 1-12.000.

71 Id.

be difficult for agencies to effectively communicate and coordinate on a particular investigation such that multi-agency resolutions are reached simultaneously. In this regard, a company that co-operates with all of the relevant government agencies could play a role in encouraging agencies to coordinate by ensuring they are aware of each agency's progress in the investigation and settlement discussions, and encouraging agencies to communicate, when appropriate.

See Chapter 24 on negotiating global settlements

10.3.2 Cross-border coordination

Coordination between international law enforcement agencies has only grown in recent years. In 2018, the DOJ announced that FCPA cases typically involve between four and five different international agencies, particularly because many of the largest DOJ bribery cases target foreign companies in coordination with foreign authorities.[72]

Cross-border investigations may present special challenges and opportunities in comparison to single-jurisdiction investigations. A recent trend apparent in large, corporate investigations is the increased level of coordination and co-operation between various law enforcement agencies. This coordination may come in the form of official, administrative channels such as mutual legal assistance treaties (MLATs), memoranda of understanding, or specific agreements between countries in relation to particular subjects.[73]

The MLAT process has undergone significant reform in recent years, in response to the oft-criticised laborious nature of preparing the requests and having them fulfilled. In December 2017, the US Attorney General called on the international law enforcement community to 'expedite mutual legal assistance requests', stating: 'If [requests for information are] not properly shared between nations, then, in many cases, justice cannot be done. It is essential that we continue to improve that kind of sharing.'[74] In accordance with this commitment to improve information sharing between the DOJ and other international law enforcement agencies, the DOJ has (1) allocated increased resources to the office responsible for handing MLAT requests and (2) established a cyber unit to process requests for electronic evidence.

In addition to these formal channels, however, international law enforcement agencies may also informally choose to share investigative strategies, information and access to information and witnesses within their respective jurisdictions. One notable innovation has been the use of text messaging between various

72 Evan Norris, 'How Enforcement Authorities Interact', Global Investigations Review (19 August 2019), available at https://globalinvestigationsreview.com/chapter/1196461/how-enforcement-authorities-interact.

73 Id.

74 Jeff Sessions, Attorney General, 'Attorney General Sessions Delivers Remarks at the Global Forum on Asset Recovery Hosted by the United States and the United Kingdom' (4 December 2017), available at https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-global-forum-asset-recovery-hosted-united.

prosecutorial agencies to compare evidence and coordinate simultaneous raids.[75] For example, in 2016, Brazilian and French prosecutors used WhatsApp to communicate in advance of the raids in the 2016 Rio Olympic Games.[76] Informal coordination presents obvious upsides to the US government. Instead of relying on slow, burdensome and languorous official processes for co-operation, informal co-operation allows US authorities to gain the benefits of shared knowledge in an expedient manner, more akin to the fast-paced nature of the wrongdoer's misconduct in large, complex cross-border investigations.

For companies, this increased co-operation changes the calculus of whether and how to co-operate with authorities, precisely because information that is shared in one jurisdiction may easily and quickly become known in another jurisdiction, potentially with different criteria for liability.

See Chapter 11 on production of information to authorities

DOJ's policy against 'piling on' 10.3.3

Given the number of different government agencies, both foreign and domestic, that could have an interest in any given investigation, in May 2018, Deputy Attorney General Rod Rosenstein announced the DOJ's new policy against 'piling on', which favours a less aggressive approach to cumulative prosecution. In describing this new policy, Rosenstein stated that that the DOJ should 'discourage disproportionate enforcement of laws by multiple authorities', likening it to the football practice of multiple players 'piling on' after a player has already been tackled.[77] He added: 'Our new policy discourages "piling on" by instructing Department [of Justice] components to appropriately coordinate with one another and with other enforcement agencies in imposing multiple penalties on a company in relation to investigations of the same misconduct', noting that often large, regulated companies are accountable to 'multiple regulatory bodies', which created the risk of duplicative and onerous punishments beyond 'what is necessary to rectify the harm and deter future violations'.[78]

Piling on can negatively affect the morale of companies, investors and customers and often can mean that companies seldom have a sense of finality when it comes to investigations by an alphabet soup of different law enforcement agencies or regulatory agencies.

Under this new policy, the DOJ now considers 'the totality of fines, penalties, and/or forfeiture imposed by' all enforcement agencies to avoid excessive punishment. Moreover, Rosenstein emphasised that the new policy reinforces the following core policies: ensuring that the federal government (1) does not

75 Evan Norris, 'How Enforcement Authorities Interact', Global Investigations Review (19 August 2019), available at https://globalinvestigationsreview.com/chapter/1196461/how-enforcement-authorities-interact.

76 See Clara Hudson, 'GIR Live: Brazilian prosecutor says WhatsApp chat group drove investigation forward', GIR (27 October 2017).

77 Rod J Rosenstein, Deputy Att'y Gen., US Dep't of Justice, Remarks to the New York City Bar White Collar Crime Institute (9 May 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

78 Id.

use its enforcement power for impermissible purposes (i.e., leveraging the threat of criminal prosecution to induce a company to settle a civil case), (2) encourages intra-governmental coordination to ensure an 'overall equitable result', (3) encourages DOJ officials to coordinate with other DOJ officials, and (4) specifies concrete factors that the DOJ will evaluate in the event that a case does warrant multiple policies.

In the enforcement of the FCPA, in particular, it has been long-standing practice for the DOJ and SEC to coordinate their investigations and ensuing resolutions; however, the formalisation of the anti-piling-on policy indicates that this practice will become more commonplace in other legal arenas.

It remains to be seen whether companies can successfully use the DOJ's anti-piling-on policy to defend against perceived duplicative charges by various government agencies. Volkswagen, the car manufacturer facing charges by the SEC for failing to disclose its clean diesel emission cheating scheme in a recent bond offering, has argued that the SEC cannot 'pile on' more charges after the company had already pleaded guilty to three felonies and paid US$25 billion in fines, penalties and settlements to US and state authorities, as well as car owners and dealers, in connection to the alleged misconduct.[79] Indeed, the judge presiding over the case has questioned why the SEC brought its case against Volkswagen two years after the company resolved the matter with the DOJ.[80] In addition, the judge acknowledged that it might be possible for Volkswagen's penalty in the SEC case to be reduced in light of the penalties the company has already paid.[81] The judge has strongly encouraged the parties to settle the case.[82]

79 Linda Chan, SEC, VW Must Cut Deal In Emissions Fraud Suit, Judge Says (16 August 2019), available at https://www.law360.com/articles/1189726/sec-vw-must-cut-deal-in-emissions-fraud-suit-judge-says.

80 David Shepardson, US Judge Urges VW, SEC to Resolve Civil Dieselgate Suit (16 August 2019), available at https://www.reuters.com/article/us-volkswagen-emissions/u-s-judge-urges-vw-sec-to-resolve-civil-dieselgate-suit-idUSKCN1V61SN.

81 Id.

82 Id.

11

Production of Information to the Authorities

Hector Gonzalez, Rebecca Kahan Waldman, Caroline Black and Lisa Foley[1]

Introduction 11.1

There are many situations in which a company may face a choice, or a demand, to disclose documents and information to a law enforcement authority or regulator. These range from responding to a raid on corporate and individual premises, to compliance with a subpoena or other compulsory process, to the voluntary provision of information during a self-disclosure. The types of information and the circumstances in which a company is obliged – or even able – to produce relevant documents is circumscribed by various laws. For example, a company must address concerns regarding confidentiality, employee privacy, data protection and legal privilege (and, in certain jurisdictions, bank secrecy restrictions or blocking statutes). This becomes additionally complicated in cross-border cases where multiple legal regimes may apply and may conflict with one another. Add to this the not uncommon scenario of authorities from different countries seeking the same (or slightly different) information and it becomes a legal and practical minefield. This chapter cannot hope to cover the immense number of variables that a company may face in these circumstances, but it does seek to provide practical guidance on some of the most important points.

1 Hector Gonzalez, Rebecca Kahan Waldman and Caroline Black are partners and Lisa Foley is an associate at Dechert LLP.

11.2 Production of documents to the authorities

11.2.1 Formal requests for disclosure (and related document hold issues)

11.2.1.1 Commonly used powers (UK)

Most regulatory and enforcement authorities have formal powers to compel individuals and companies to produce documents and provide information.

In the area of financial crime and corruption involving the United Kingdom, the most likely authority to be seeking to investigate and prosecute will be the Serious Fraud Office (SFO). It has powers to seek the production of documents and information at both a pre-investigation stage in relation to bribery and corruption cases under section 2A of the Criminal Justice Act 1987, and, once it opens a formal investigation, under section 2 of the same Act. These powers can be exercised against companies and individuals to produce documents and information, including by way of compelled interview where there is no right to silence (although the individual cannot be later prosecuted regarding matters arising from the interview, unless the information is found to be false). A failure to provide the documents and information within the time specified in the production notice is a criminal offence, unless the recipient can show that it had a reasonable excuse not to comply (such as an injunction preventing production).

In the field of financial markets regulation, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) have powers to compel the production of documents, contained in Part 11 of the Financial Services and Markets Act 2000 (FSMA). The key provision is section 165, subsections 1 to 6 of which are set out below as an example of how information-gathering powers are conferred:

> *165 Regulators' power to require information: authorised persons etc.*
> *(1) Either regulator may, by notice in writing given to an authorised person, require him–*
> *(a) to provide specified information or information of a specified description; or*
> *(b) to produce specified documents or documents of a specified description.*
> *(2) The information or documents must be provided or produced–*
> *(a) before the end of such reasonable period as may be specified; and*
> *(b) at such place as may be specified.*
> *(3) An officer who has written authorisation from the regulator to do so may require an authorised person without delay–*
> *(a) to provide the officer with specified information or information of a specified description; or*
> *(b) to produce to him specified documents or documents of a specified description.*
> *(4) This section applies only to–*
> *(a) information and documents reasonably required in connection with the exercise by either regulator of functions conferred on it by or under this Act; and*

> *(b) in relation to the exercise by the PRA of the powers conferred by subsections (1) and (3), information and documents reasonably required by the Bank of England in connection with the exercise by the Bank of its functions in pursuance of its financial stability objective.*
>
> *(5) The regulator in question may require any information provided under this section to be provided in such form as it may reasonably require.*
>
> *(6) The regulator in question may require–*
>
> *(a) any information provided, whether in a document or otherwise, to be verified in such manner; or*
>
> *(b) any document produced to be authenticated in such manner, as it may reasonably require.*

'Authorised person' is defined in section 31 of the FSMA and means, very broadly, a person providing a regulated financial service.

The FCA has set out its policy in relation to its exercise of enforcement powers under the FSMA (and other legislation) in its Enforcement Guide and the FCA's report on its approach to enforcement.[2] The Enforcement Guide is useful as it not only sets out the FCA's approach to its task as the United Kingdom's financial markets regulator, but also it reflects the general approach of UK regulators to their document production powers.

In paragraph 4.7 of the Enforcement Guide, the FCA states that its standard practice is to use its statutory powers to require the production of documents, the provision of information or the answering of questions in interview. The FCA suggests that this is for reasons of fairness, transparency and efficiency. The Enforcement Guide goes on to suggest, however, that it will sometimes be appropriate to depart from this standard practice, as it relates to document production, for example in cases:

- involving third parties with no professional connection with the financial services industry, such as the victims of an alleged fraud or misconduct, in which case the FCA will usually seek information voluntarily;
- where the FCA has been asked by an overseas or EEA regulator to obtain documents on their behalf, in which case the FCA will discuss with the overseas regulator the most appropriate approach.

In the second scenario, it is important to consider the effect of regimes and jurisdictional protections colliding. For example, how might the US right to silence mesh with the UK compelled disclosure regime? The Enforcement Guide states that the FCA will make it clear to the company or individual concerned whether

2 Financial Conduct Authority (FCA), Enforcement Guide (January 2016), available at https://www.handbook.fca.org.uk/handbook/EG/; and FCA Mission: Approach to Enforcement (April 2019), available at https://www.fca.org.uk/publication/corporate/our-approach-enforcement-final-report-feedback-statement.pdf.

See Chapters 15 and 16 on representing individuals in interviews and Chapters 17 and 18 on individuals in cross-border proceedings

it requires him, her or it to produce information or answer questions under the FSMA or whether the provision of information is voluntary.[3]

Similar (but unique) powers also lie in the hands of the Competition and Markets Authority, the National Crime Agency, the police, Her Majesty's Revenue and Customs, and the Health and Safety Executive. Many of these authorities may also apply for and obtain search warrants and use these powers more often than their US counterparts do.

11.2.1.2 Commonly used powers (US)

In the United States, most federal agencies, including the United States Department of Justice (DOJ), the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) may issue subpoenas (or administrative orders) and compel individuals and companies to produce documents and testimony.[4] In the case of the DOJ, a subpoena may compel the production of documents in connection with either a civil or criminal investigation.[5] The CFTC's regulations provide that:

> *The Commission or any member of the Commission or of its staff who, by order of the Commission, has been authorized to issue subpoenas in the course of a particular investigation may issue a subpoena directing the person named therein to appear before a designated person at a specified time and place to testify or to produce documentary evidence, or both, relating to any matter under investigation.*[6]

Additionally, state agencies and each state's attorney general can compel the production of documents and testimony. As an example, Section 352 of the New York General Business Law permits the Attorney General to commence an investigation of an individual or corporation and to seek documents and testimony in connection with that investigation. The Securities Act, the Securities Exchange Act, the Investment Advisers Act and the Investment Company Act all permit the SEC to issue subpoenas in connection with an ongoing investigation of misconduct.[7]

---

3 Whether the FCA compels testimony from an individual can have an impact on whether that information can be used in connection with a criminal proceeding in the United States. The Second Circuit Court of Appeals has held that testimony compelled by the FCA cannot be used against a defendant in a criminal prosecution. See *United States v. Allen*, 864 F.3d 63 (2d Cir. 2017).

4 Other federal agencies, such as the Consumer Financial Protection Bureau and the Federal Trade Commission, are authorised to issue subpoenas. Other agencies are required to seek the assistance of the United States Attorney's Office in seeking documents and testimony. For a discussion of the use of administrative subpoenas, see www.justice.gov/archive/olp/rpt_to_congress.htm.

5 For information regarding criminal matters, see Justice Manual § 9-13. The Civil Division is authorised to issue subpoenas by a number of statutes.

6 17 C.F.R. § 11.4(a).

7 Section 19(c) of the Securities Act of 1933, 15 U.S.C. § 77s(c); Section 21(b) of the Securities Exchange Act of 1934, 15 U.S.C. § 78u(b); Section 209(b) of the Investment Advisers Act

Before a subpoena can be issued, the staff of the SEC must obtain a formal order of investigation.[8]

Criminal offences for refusing to comply with a request, providing false or misleading statements, or concealing documents, generally supplement such powers.[9]

Scope and timing 11.2.1.3

In practice, a company can do little to resist complying with a formal request for disclosure without resorting to court proceedings to challenge the validity or scope of the request. However, it can likely negotiate with the relevant authority regarding the scope of documents responsive to the request and the production date to limit the scope of the request to what is proportionate and reasonable.

Broadly drawn requests are unfortunately not uncommon, as investigators seek to ensure the requests will capture all relevant information. Early engagement with the relevant authority will typically ensure that both parties can agree on scope and a timetable for production: a request looking back over a long period, or even without any time limit, could involve a lengthy resource-intensive review and expensive production exercise. This may not be in the interests of the prosecuting agency or the company if a more targeted request could produce the information. Whether an agreement to narrow the scope of the request is possible is likely to depend, in large part, on factors outside the company's control – such as the nature and scope of the authority's investigation (which the authority may be unwilling to share and is likely to base on information and evidence outside the company's knowledge). However, the company and its legal advisers should nonetheless seek a reasonable, proportionate and practically achievable production: for example, by seeking to agree to produce documents relating to X project, between Y and Z dates and if necessary to produce the documents in tranches.

It becomes increasingly difficult to manage the response to multiple authorities, particularly if they are in different countries and have different areas of focus. Similarly, a company must consider whether the production notice extends to materials held overseas.

For responding to broad document requests involving large volumes of data, a company may decide to use artificial intelligence or technology assisted review (TAR) to improve the accuracy and speed within which relevant documents are identified. This is becoming increasingly accepted in the United Kingdom. The

---

of 1940, 15 U.S.C. § 80b–9(b); and Section 42(b) of the Investment Company Act of 1940, 15 U.S.C. § 80a–41(b).

8 For information regarding procedures for obtaining a formal order of investigation, see sections 2.2.3 to 2.3.4 of the Enforcement Manual of the Securities and Exchange Commission Division of Enforcement, available at https://www.sec.gov/divisions/enforce/enforcementmanual.pdf (28 November 2017).

9 18 U.S.C. §§ 401, 1001; see also 7 U.S.C. §§ 9, 13(a)(3). Rule 17 of the Federal Rules of Criminal Procedures, governs subpoenas, including grand jury subpoenas and Rule 17(g) authorises federal courts to exercise its contempt powers for non-compliance. ('The court (other than a magistrate judge) may hold in contempt a witness who, without adequate excuse, disobeys a subpoena issued by a federal court in that district.')

SFO confirmed its use of artificial intelligence technology in the deferred prosecution agreement (DPA) case of *SFO v. Rolls-Royce PLC*.[10]

In the United States, while TAR might be used appropriately in responding to subpoenas or document requests in some limited instances, its use would likely be subject to an agreement regarding its use with the requesting agency.

11.2.1.4 Practical steps on receipt

Upon receipt of a document request, a company should – in most cases – immediately issue a document retention (or hold) notice (DRN) (if one is not already in place). A company should take care not to inadvertently tip off data custodians, who may also be suspects. In some cases, issuing a DRN is not appropriate; for example, where the company is investigating matters outside the public domain and needs to collect documents covertly at the outset. The issuing of a DRN will assist the company to demonstrate that it has taken steps to preserve all potentially relevant documents in existence at the date of the request. The DRN should track the terms of the production notice, and be sent to all personnel who may have responsive documents, including the IT department and records department. The term 'document' should be widely drawn to include any paper or electronic records present on any media (including instant messaging applications) belonging to the company or its employees, including corporate information located off-site. The company may also need to manage complicated issues around data privacy and personal media.[11]

See Chapters 13 and 14 on employee rights and Chapter 40 on data protection

The DRN should confirm that employees must not delete, alter, conceal or otherwise destroy company documents. Simultaneously, the company should take steps to secure and preserve all relevant information held on the company's servers and backup tapes, including through external providers. It should also immediately suspend routine document and data destruction processes.

Most authorities will have their own technical standards, which the collection and production of electronically stored information must meet. It is therefore likely that a company seeking to respond to a subpoena or production notice will want to consider instructing a forensic IT specialist company to assist with the collection and production efforts. This will have the added benefit of ensuring that a company can demonstrate the independence of this analysis, that it is taking

10 *Serious Fraud Office v. Rolls-Royce PLC and Rolls-Royce Energy Systems Inc* (Case No. U20170036) [2017] Lloyd's Rep FC 249.

11 For example, employees' use of disappearing messaging services, such as WhatsApp, raises issues. In March 2019, the Department of Justice (DOJ) relaxed its prior guidance to companies regarding employees' use of those services, removing from the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy a requirement that employees be prohibited from using those services. Instead, the revised policy requires that each company seeking timely and appropriate remediation credit 'appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations.' Justice Manual § 9-47.120.

clear co-operative steps, and protects employees, as far as possible, from having to give evidence in any subsequent proceedings.

Informal requests for disclosure: voluntary production and co-operation 11.2.2

A company may wish to consider voluntarily providing documents to an authority as part of a self-report or to demonstrate its co-operation with an investigation. Government investigators and investigating authorities regularly hold out the possibility of co-operation credit to companies to encourage them to provide information about their own misconduct.

From February 2014, DPAs have been available in the United Kingdom to the SFO and Crown Prosecution Service for disposing of corporate criminal conduct relating broadly to economic crime (including, in particular, fraud, corruption and money laundering).[12] The SFO and the English courts have emphasised that one of the most important factors for a DPA is early reporting and co-operation by the company. Co-operation should be 'genuinely proactive'.[13] This includes the voluntary production of relevant documents, the importance of which has been demonstrated in one of the early DPA cases of *SFO v. Rolls-Royce PLC*,[14] discussed later in this chapter. In the United Kingdom, the Director of the SFO since August 2018, Lisa Osofsky, has explained that corporate co-operation means 'making the path to a case easier' for the prosecutor.[15] This means that companies will be expected to provide the SFO with evidence it does not already have and guide the SFO's investigation to help it focus on the most relevant lines of enquiry, including in respect of assistance with future prosecutions of individuals.

In August 2019, the SFO updated its Operational Handbook to provide guidance on corporate co-operation (Corporate Co-operation Guidance), confirming a non-exhaustive list of good practices that SFO officers should consider when assessing an organisation's co-operation with the SFO, with a view to potentially being offered an invitation to enter into DPA negotiations. The Corporate Co-operation Guidance sets forth detailed provisions on the SFO's expectations regarding the preservation and provision of materials relating to digital and hard-copy evidence, financial records and analysis, industry and background information, dealing with individuals connected to the investigation, and more contentious issues such as witness accounts and waivers of privilege. The

12 Deferred prosecution agreements (DPAs) were introduced by s.45 and Sch. 17 of the Crime and Courts Act 2013.

13 Crown Prosecution Service and Serious Fraud Office, Deferred Prosecution Agreements Code of Practice – Crime and Courts Act 2013, 11 February 2014, at para. 2.8.2(i).

14 *Serious Fraud Office v. Rolls-Royce PLC and Rolls-Royce Energy Systems Inc* (Case No. U20170036) [2017] Lloyd's Rep FC 249. Rolls-Royce first came to the attention of the Serious Fraud Office (SFO) in early 2012, when a whistleblower raised concerns about Rolls-Royce's business in China and Indonesia. After a lengthy investigation, Rolls-Royce accepted responsibility for criminal offending over 24 years, in seven different countries. Ultimately, Rolls-Royce was granted a DPA, and paid approximately £800 million in financial penalties to authorities in the United Kingdom, United States and Brazil.

15 See https://www.sfo.gov.uk/2018/12/04/keynote-address-fcpa-conference-washington-dc/.

Corporate Co-operation Guidance confirms that 'cooperation means providing assistance to the SFO that goes above and beyond what the law requires' and that this includes identifying individuals involved in the misconduct.[16]

In the United States, too, the authorities have routinely emphasised that they will consider self-reporting and co-operation with government investigations as a key factor when determining whether to charge a corporation.[17] The DOJ encourages corporations to conduct internal investigations and voluntarily self-report misconduct.[18] The Justice Manual states that prosecutors may consider voluntary disclosure when determining whether to bring charges for criminal misconduct.[19] Under the DOJ's Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy, which has been incorporated into the Justice Manual:

> *[W]hen a company has voluntarily self-disclosed misconduct in an FCPA matter, fully cooperated, and timely and appropriately remediated, all in accordance with the standards set forth below, there will be a presumption that the company will receive a declination absent aggravating circumstances involving the seriousness of the offense or the nature of the offender.*[20]

Importantly, voluntary disclosure is just one factor that is considered in determining whether to bring an action against the corporation.[21] In November 2019, the DOJ revised its definition of 'voluntary self-disclosure' in FCPA matters.[22] To receive credit for voluntary self-disclosure, a company will need to disclose 'all relevant facts known to it at the time of disclosure, including as to any individuals substantially involved in or responsible for the misconduct at issue'.[23] These changes were necessary to harmonise the standards of the Corporate Enforcement Policy with prior guidance by the DOJ and to acknowledge that a company might not be in a position to know the full extent of wrongdoing at the time of the initial disclosure.[24] The Corporate Enforcement Policy does provide benefits to a company that does not voluntarily self-disclose misconduct but does fully co-operate with an investigation and implement timely and appropriate remediation.[25]

16 Corporate Co-operation Guidance, SFO Operational Handbook (6 August 2019).

17 See, e.g., memorandum dated 5 July 2007 from Paul J McNulty re Principles of Federal Prosecution of Business Organizations available at https://www.justice.gov/sites/default/files/dag/legacy/2007/07/05/mcnulty_memo.pdf.

18 Justice Manual §§ 9-28.900, 9-47.120.

19 Justice Manual § 9-28.900. ('Even in the absence of a formal program, prosecutors may consider a corporation's timely and voluntary disclosure, both as an independent factor and in evaluating the company's overall co-operation and the adequacy of the corporation's compliance program and its management's commitment to the compliance program.')

20 See Justice Manual § 9-47.120.

21 Justice Manual §§ 9-28.300, 9-28.900, 9-47.120.

22 Justice Manual § 9-47.120.

23 Justice Manual § 9-47.120.

24 Justice Manual § 9-47.120 at note 1.

25 Justice Manual §§ 9-28.300, 9-28.900; see also https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-34th-international-conference-foreign.

Timing is important, both for a potential DPA and in relation to anti-cartel regimes, which often provide an amnesty only to the first discloser.[26]

As has been noted above, the FCA's standard practice is to rely on its statutory powers to require the production of documents. While there is merit in adopting this policy, and it does avoid the risks to companies of voluntarily disclosing documents to the FCA set out below, nothing prevents the FCA from seeking voluntary production. Principle 11 of the FCA's Principles for Businesses states: 'A firm must deal with its regulators in an open and co-operative way, and must disclose to the appropriate regulator appropriately anything relating to the firm of which that regulator would reasonably expect notice.' A materially identical provision is included in the PRA's Rulebook as Fundamental Rule 7. While this chapter focuses on the approach of the FCA, it is worth remembering that the PRA has similar enforcement powers (and is using them with increasing frequency). Both regulators interpret these obligations to proactively bring matters to their attention widely, and are prepared to take enforcement action against firms and individuals for failures to discharge these obligations (even in the absence of other underlying failings). Prudential Group (fined £30 million for failing to inform the Financial Services Authority (FSA)[27] of its proposed acquisition of AIA until after it had been leaked to the media), Goldman Sachs (fined £17.5 million for not disclosing an SEC investigation into its staff and members of The Goldman Sachs Group), the Co-operative Bank (issued a final notice for failing to notify the PRA without delay of two intended personnel changes in senior positions) and Bank of Scotland plc (fined £45.5 million for failure to inform the FSA about its suspicions that fraud may have occurred at the Reading-based impaired assets team of Halifax Bank of Scotland) are recent examples. This places regulated firms in a different position from other corporates: it reduces the scope for the decision whether to self-report or not.

Principle 11 is mainly intended as a supervision tool and sets out a broad duty of co-operation that the FCA often relies on to oblige the production of documents prior to formal investigations being commenced (sometimes, but not always, for the purpose of deciding whether an investigation should be commenced and, if so, in respect of which firms and individuals). The FCA's view of what is meant by being open and co-operative within Principle 11 is set out in the FCA Handbook, in the 'Supervision' section (referred to as SUP). SUP 2.3 provides that 'open and co-operative' includes a regulated entity making itself readily available for meetings with the FCA, giving the FCA reasonable access to records, producing documents as requested, and answering questions truthfully, fully and promptly. Where a formal investigation has been commenced, the FCA would not seek to rely on Principle 11 as a substitute for its other statutory powers that compel production. While it would be a clear breach of Principle 11 to fail to comply with a statutory request for the production of documents, a failure to

26 See, e.g., European Commission Notice on Immunity from Fines and Reduction of Fines in Cartel Cases, Official Journal C 298, 8 December 2006, p. 17.

27 The Financial Services Authority was the predecessor to the FCA.

comply with a voluntary request for the production of documents would not, of itself, result in disciplinary proceedings. The Enforcement Guide does state, in the context of co-operation, that:

> *The FCA will not bring disciplinary proceedings against a person for failing to be open and co-operative with the FCA simply because, during an investigation, they choose not to attend or answer questions at a purely voluntary interview. However, there may be circumstances in which an adverse inference may be drawn from the reluctance of a person (whether or not they are a firm or individual) to participate in a voluntary interview. If a person provides the FCA with misleading or untrue information, the FCA may consider taking action against them.*[28]

The Enforcement Guide further provides that if a person does not comply with a requirement imposed by the exercise of statutory powers, he or she may be held to be in contempt of court. The FCA may also choose to bring proceedings for breach of Principle 11.[29] Therefore, while there is no guidance indicating that a failure to produce documents voluntarily (as opposed to attending a voluntary interview) would result in an adverse inference being drawn, a decision by a company not to produce documents voluntarily in any particular case should not be made without careful forethought and proper advice on the potential consequences.

As this suggests, the Enforcement Guide recognises the importance of an open and co-operative relationship with the firms it regulates to the effective regulation of the UK financial system. When deciding whether to exercise its enforcement powers, the FCA considers, among a number of factors, the level of co-operation demonstrated by a firm. When weighing the level of co-operation, the FCA considers whether the firm has been open and communicative with it.

Voluntarily disclosing documents carries a risk that the authority may not give any meaningful credit and may nonetheless decide to prosecute or expand an investigation already under way. Therefore, the company should weigh the likelihood of the authority being able to serve a formal request for disclosure in the relevant jurisdiction.

See Section 11.2.4.6, and Chapters 35 and 36 on privilege

In some instances, a formal notice for disclosure will be preferred: for example, where a company has obligations of confidentiality, preventing voluntary disclosure. The most common examples are lawyers and financial institutions, who could both face an action for breach of confidence for supplying documents or information without a formal regulatory request. In some self-reporting circumstances, it may be appropriate for a company to seek such a notice from the relevant authority to ensure that it does not open itself up to civil action. The notice should be narrowly drawn, in consultation with the regulator, and should not affect the company's co-operation credit. Likewise, in some situations, the company may prefer to ask to be provided with a formal document request to

28 See Enforcement Guide, at para. 4.7.3.

29 Enforcement Guide, at para. 4.7.4.

demonstrate that they have been compelled to produce the documents to the authorities and have not done so voluntarily.

Production of information to multiple authorities 11.2.3

The increasingly complex and multi-jurisdictional nature of investigations means that a company may face requests for formal disclosure from more than one authority. These could be authorities with different mandates within the same jurisdiction, or authorities with similar mandates from different jurisdictions. In either case, multi-authority investigations demand holistic strategies and systems to allow a company to keep track of evidence disclosed to (or seized by) different authorities. A company may also want to consider if there is any strategic advantage to disclosing to one authority before another. However, recent large-scale global investigations into the manipulation of LIBOR and foreign exchange rates demonstrate the ever increasing levels of intra- and international co-operation between regulators.[30] Practical steps a company can take when faced with multiple requests for formal disclosure include:

- early engagement with each authority, to communicate expectations and practical difficulties of responding to multiple requests;
- identifying and prioritising information that is commonly responsive to the requests rather than focusing on responding to each individual request in isolation;
- maintaining clear production schedules; and
- ensuring a system for Bates numbering[31] for each authority.

Documents and data outside the jurisdiction 11.2.4

Voluntary production 11.2.4.1

In cross-border fraud or corruption cases, not all of a company's documents will be located or even accessible in the same jurisdiction as the investigating authority. In assessing timely disclosure of documents in connection with obtaining credit for 'Full Cooperation in FCPA Matters', the DOJ will consider 'disclosure of overseas documents, the locations in which such documents were found, and who found the documents'.[32] Importantly '[w]here a company claims that disclosure of overseas documents is prohibited due to data privacy, blocking statutes, or other reasons related to foreign law, the company bears the burden of establishing the prohibition. Moreover, a company should work diligently to identify all available

30 In 2015, Deutsche Bank AG entered into a DPA with the DOJ and settlements with the US Commodity Futures Trading Commission, the Department of Financial Services and the FCA, in connection with its role in manipulating LIBOR rates. DB Group, a subsidiary of Deutsche Bank, also pleaded guilty to wire fraud for its role. Together, Deutsche Bank and its subsidiary agreed to pay over US$2 billion in penalties to US authorities and US$344 million to the FCA – then the second-largest fine in the FCA's history.

31 Bates numbering is a method of indexing legal documents for easy identification and retrieval.

32 Justice Manual §9-47.120(3)(b).

legal bases to provide such documents'.[33] A company should consider what documents are stored overseas, and which of these it should provide to investigators. Recent judicial decisions have furthered the powers of UK authorities to obtain information located outside the jurisdiction for the purposes of an investigation, and the Corporate Co-operation Guidance confirms that co-operating organisations should supply relevant material that is held abroad, where it is in the possession or control of the organisation. A company in receipt of a formal production notice will need to assess whether the notice extends to documents outside the jurisdiction and, if so, the extent to which the company has 'custody or control' over documents held by subsidiaries or overseas branches.[34] The board of a parent company will not necessarily control the management of a subsidiary.[35]

The Corporate Co-operation Guidance also confirms that the SFO will expect co-operating organisations to identify relevant material in the possession of third parties and assist the SFO in obtaining it. Companies should also inform the SFO about relevant material that the company is unable to access (such as messaging apps and bank accounts).

Where production is voluntary, a company may take a more holistic view of the investigation and production (subject to local law restrictions). The extent to which it may want to voluntarily disclose information may depend on the ability of the investigating authority to obtain that information itself. However, given the increasing co-operation between authorities on the international stage, careful voluntary production of material is likely to be preferable, and vital if the company seeks co-operation credit. As previously noted, to receive credit for full cooperation under the FCPA Corporate Enforcement Policy, a company cannot simply refuse to produce certain documents on the basis that production is prohibited by rule or regulation. Rather, the company 'bears the burden of establishing the

33 Justice Manual §9-47.120(3)(b).

34 Production notices seeking documents held outside the jurisdiction of the investigating authority are complicated. For example, the authors take the view that a request made under s.165 of the Financial Services and Markets Act 2000 captures documents in a company's custody or control outside the United Kingdom. In the 2018 case of *R (on the Application of KBR Inc) v. The Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), the High Court held that the SFO's compulsory document production powers under section 2(3) of the Criminal Justice Act 1987 could have extraterritorial application, but to issue a notice to a non-UK company in respect of documents held outside the United Kingdom, there must be a 'sufficient connection' between the overseas company and the United Kingdom. Overseas companies should assess the factual connection to the United Kingdom (in terms of its connection to the subject matter of the SFO's investigation), rather than from a business perspective. The UK Supreme Court has granted KBR leave to appeal this decision. In the case of *R (on the application of Tony Michael Jimenez) v. (1) First Tier Tax Tribunal and (2) Her Majesty's Commissioners for Revenue and Customs* [2019] Civ 51, the Court of Appeal applied the 'sufficient connection' test set out in *KBR* in determining that HM Revenue and Customs, the UK tax authority, is authorised to serve a 'taxpayer notice' on a UK taxpayer resident overseas to obtain information about that individual's tax position.

35 For the United Kingdom, see *Lonrho v. Shell Petroleum* [1980] 1 WLR 627.

prohibition' and 'should work diligently to identify all available legal bases to provide such documents'.[36]

Mutual legal assistance 11.2.4.2

In the United Kingdom, sections 7 to 9 of the Crime (International Co-operation) Act 2003 (CICA) govern requests to obtain evidence from abroad in relation to a prosecution or investigation taking place in the United Kingdom, shaping the mutual legal assistance (MLA) powers of UK authorities. Under CICA, an MLA request can only be made if it appears to the investigating authority that an offence has been committed or there are reasonable grounds for suspecting that an offence has been committed, and either proceedings in respect of that offence have been instituted or the offence is being investigated.[37] The request must relate to the obtaining of evidence 'for use in the proceedings or investigation'.[38] But, it could allow an investigating agency to have foreign law enforcement officers launch raids, arrest suspects or conduct interviews on its behalf.[39] If the implementation of an MLA request in the requested state requires a court order, then the court in the requested state is likely to apply the relevant principles in its own jurisdiction to satisfy itself that the requested order is justified.

Note that among the vast majority of EU Member States, European investigation orders (EIOs) now allow streamlined access to evidence and information in criminal investigations. EIOs work on the basis of mutual recognition, and judicial authorities can use them to request assistance with 'any investigative measure' (although the EIO itself will identify a number of investigative activities that it does not permit). More specifically, the EIO:

- replaces the previous fragmented legal framework for obtaining evidence within Europe by providing a single instrument;
- imposes a strict 30-day deadline for the Member State to accept the request, and 90 days to comply;
- limits the reasons for which the Member State can refuse the request;
- introduces a standard form; and
- prioritises the necessity and proportionality of the measure as part of the rights of the defence.

EIOs were created by EU Directive 2014/41/EU, which came into force in the United Kingdom on 31 July 2017 (transposed through the Criminal Justice (European Investigation Order) Regulations 2017). The United Kingdom has opted into the EIO regime even though it has chosen to exit the European Union.

In April 2018, the European Commission issued a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal

36 See Justice Manual § 9-47.120.

37 Crime (International Co-operation) Act 2003, s.7(5).

38 Crime (International Co-operation) Act 2003, s.7(2).

39 See, e.g., Reuters, 'Monaco raids Unaoil offices over global oil corruption probe', available at http://uk.reuters.com/article/uk-oil-companies-corruption-idUKKCN0WY3KM.

matters.[40] The proposal aims to reform cross-border access to electronic evidence and make MLA across Member States more efficient. It would allow Member States to request electronic evidence directly from service providers established or represented in a Member State that provide services in the European Union (regardless of the location of the data requested). The regulation would require the service provider to respond within 10 days or, in cases of emergency, six hours.

In December 2018, the Council of the European Union agreed its position on the proposal, which is currently with a European Parliament committee.[41] The United Kingdom has decided not to opt into the proposal, stating that 'it is not clear how new EU legislation will be a practical and effective way to address the global issue of providing lawful access to data held anywhere in the world'.[42]

In February 2019, the UK Parliament passed its own legislation on cross-border access to electronic evidence, the Crime (Overseas Production Orders) Act 2019. This new legislation gives UK authorities (including the SFO and FCA) the power to apply to a UK court to compel a company operating or an individual based outside the United Kingdom to provide electronic data stored abroad. This new law allows UK authorities to sidestep the notoriously slow process of seeking MLA in favour of obtaining an overseas production order, which can be served directly on the person storing the electronic data.[43] This legal development brings the United Kingdom into alignment with the US regime. In 2018, the US federal government passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, explicitly authorising US law enforcement agencies to obtain data held by US cloud service providers regardless of where in the world the data is physically stored. The CLOUD Act also created a framework by which foreign countries (such as the United Kingdom) could seek disclosure of data held by US cloud service providers, without US co-operation or oversight.

The MLA process can be cumbersome, but is a very real threat in the event a company does not co-operate. A company should also not overlook the significant scope for informal direct investigator-to-investigator co-operation. Agencies such as Interpol have dedicated programmes to share information between, and support investigations by, investigating agencies in different countries. Communications between the SFO and DOJ are frequent. The FCA, specifically, has a broad discretion to assist foreign regulators. This discretion is set out in section 169 of the FSMA. The statutory power is supplemented by relevant FCA

40 See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN.

41 See https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2018/0108(COD).

42 http://europeanmemoranda.cabinetoffice.gov.uk/files/2018/10/HOC_Letter_Opt-in_Decision_.pdf.

43 Overseas production orders (OPOs) will only be available where the United Kingdom has a 'designated international co-operation agreement' (DICA) with the country in which the OPO will be served. The United States and the United Kingdom have been negotiating such an agreement since 2015. This means that the United States is likely to be the first country directly affected by OPOs. The fact that a DICA is a precondition of an OPO means we are unlikely to see OPOs in practice in the immediate future.

policy. Subsection 169(4) sets out the considerations in the FCA's decision as to whether to assist a foreign regulator. It provides:

> *(4) In deciding whether or not to exercise its investigative power, the regulator may take into account in particular:*
>
> *(a) whether in the country or territory of the overseas regulator concerned, corresponding assistance would be given to a United Kingdom regulatory authority;*
>
> *(b) whether the case concerns the breach of a law, or other requirement, which has no close parallel in the United Kingdom or involves the assertion of a jurisdiction not recognised by the United Kingdom;*
>
> *(c) the seriousness of the case and its importance to persons in the United Kingdom;*
>
> *(d) whether it is otherwise appropriate in the public interest to give the assistance sought.*

In an early decision on this section, *Financial Services Authority v. Amro International*,[44] the Court of Appeal held that there was nothing in section 169 that required the FCA's predecessor body to satisfy itself of the correctness of what it was being asked to investigate or gather by way of information. At the SEC's behest, the FCA could seek any document that it reasonably considered relevant to the investigation the SEC was conducting. The Court of Appeal made clear that the only requirements the FCA must meet were contained in the statute. The Court of Appeal also noted that in exercising these powers, the stricter rules attaching to the drafting of a subpoena did not apply and the description of the documents sought would be acceptable provided the recipient could identify the documents he or she was required to produce.

In addition to the FCA's statutory powers, a number of memoranda of understanding are in place between UK regulators and their overseas counterparts (most notably the SEC and other US regulators) concerning co-operation and information sharing. Recent years have seen significant co-operation between the SEC and the FCA and its cognate agencies.

Similarly, the United States has entered into mutual legal assistance treaties (MLATs) with more than 70 foreign jurisdictions, which can be used for the sharing of information and taking of evidence abroad.[45] Some US authorities also have

44 *Financial Services Authority v. Amro International* [2010] EWCA Civ 123.

45 See www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm; see also *In re Premises Located at 840 140th Ave. NE, Bellevue, Wash.*, 634 F.3d 557, 563–64 (9th Cir. 2011) ('In recent decades, the United States has ratified an increasing number of bilateral treaties with other nations to facilitate legal proceedings, known as mutual legal assistance treaties or MLATs . . . . As their names suggest, these treaties provide for bilateral, mutual assistance in the gathering of legal evidence for use by the requesting state in criminal investigations and proceedings. Viewed through the lens of reciprocity, MLATs represent a direct approach to achieving reciprocity with other nations, in addition to the indirect approach taken by congressional expansion of the scope of § 1782. The ratification of MLATs in recent decades can be seen as yet another step toward the

memoranda of understanding in place with sister agencies outside the United States, which can allow for inter-agency sharing of documents.

Recent public policy statements made by UK and US prosecuting authorities demonstrate how important they consider international co-operation to be. In the United Kingdom, SFO Director Lisa Osofsky has publicly affirmed her intention to leverage international contacts she made through her previous roles as a federal prosecutor for the DOJ and Deputy Counsel at the Federal Bureau of Investigation to strengthen the SFO's investigational capacities. As part of her oral evidence to the House of Commons Justice Committee in December 2018, she anticipated that the 'shared use of important intelligence information' would help 'crack open' cases.[46]

Ms Osofsky also confirmed that the SFO is preparing for a no-deal Brexit during her testimony before the House of Commons Justice Committee. If the United Kingdom leaves the European Union without a deal, the SFO will need to rely on pre-existing multilateral treaties for the continued sharing of information and co-operation, and could lose access to some European intelligence-sharing programmes. However, it is likely that international agencies will work together with the SFO to find workable solutions as there is a shared benefit to continuing co-operation and intelligence-sharing. Therefore, while a no-deal Brexit may slow down the process and make it more expensive, it is unlikely to stop access to European information and intelligence.

Ms Osofsky has indicated her aspiration to build on the SFO's co-operation with other agencies and civil society to share best practices. She brought in the US-qualified co-head of Jenner & Block's London investigations practice, Peter Pope, to spend a year at the SFO, to 'assist with building and consolidating relationships with authorities in other jurisdictions and to act as an adviser in case reviews and on compliance issues' according to a press release issued in September 2018.[47] Before Ms Osofsky's arrival, the DOJ had already seconded a lawyer to the SFO, enabling the exchange of ideas, experience and best practice regarding the investigation and prosecution of economic crime with the SFO's US counterpart.[48]

In the United States, the DOJ has recently adopted a 'no piling on' policy regarding penalties. This policy explicitly includes co-operation with foreign agencies. Former Deputy Attorney General, Rod Rosenstein, explained in remarks in May 2018 that the policy discourages 'disproportionate enforcement of laws by multiple authorities' by 'instructing Department components to appropriately coordinate with one another and with other enforcement agencies in

goal of greater legal assistance by, and for, other nations, at least with respect to requests by foreign governments for use in underlying criminal investigations and proceedings.').

46 Lisa Osofsky, evidence to House of Commons Justice Committee, 18 December 2018.

47 See https://www.sfo.gov.uk/2018/09/27/new-senior-roles-at-the-sfo/.

48 See https://www.sfo.gov.uk/wp-content/uploads/2019/07/SFO-Annual-Report-and-Accounts-2018-2019.pdf.

imposing multiple penalties on a company in relation to investigations of the same misconduct'.[49]

Data protection 11.2.4.3

Responding to an investigation (and conducting an internal investigation) will require data about individuals to be processed. Such an exercise will engage a number of data protection considerations.[50] A company cannot assume that complying with the data protection requirements in the investigated jurisdiction will mean compliance with overseas data protection laws. Local law may also restrict a company's ability to transfer individual data overseas. The European Union's General Data Protection Regulation (GDPR) came into force on 25 May 2018 and applies within the EU and to those data controllers and processors outside the EU who offer goods and services to EU consumers. Chapter 5 of the GDPR deals with transfers of data to third countries (and international organisations) and re-enacts existing restrictions on transferring data to countries that do not have adequate privacy protections in circumstances where other 'appropriate safeguards' are not in place. The GDPR introduces a limited derogation to its principles based on 'compelling legitimate interests', which could cover non-repetitive transfers to foreign regulators, but would require prior notification to the relevant data protection authority.

See Chapter 40 on data protection

Under the GDPR, supervisory authorities from EU Member States may issue fines of up to €20 million or 4 per cent of an organisation's global turnover from the preceding financial year (whichever is higher) for GDPR breaches. Before issuing a fine, the UK's data protection supervisory authority, the Information Commissioner's Office (ICO), must serve a written 'notice of intent' to an organisation, which allows the recipient to make representations.[51] In July 2019, the ICO issued notices of intent to fine British Airways (approximately £183 million)[52] and hotel group Marriott International (approximately £99 million)[53] for GDPR breaches. These are the first fines publicly proposed by the ICO for GDPR infringements. If ultimately issued, these fines will represent the most significant

49 See www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

50 The United States does not have a comprehensive, federal data protection law. There are, however, numerous state and federal laws that govern the treatment of personal data. At the federal level, there are protections for, among other things, data collected from children, from financial institutions and that includes medical information. See, e.g., Federal Trade Commission Act, 15 U.S.C. §§ 41 to 58; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 to 6506; Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 U.S.C. §§ 6801 to 6827; Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1301 et seq. (and the rules and regulations promulgated thereunder); Fair Credit Reporting Act, 15 U.S.C. § 1681.

51 Data Protection Act 2018 (UK implementation of GDPR), Schedule 16.

52 See https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

53 See https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

penalties ever issued by the ICO and the largest penalties imposed by any regulator to date under the GDPR. British Airways and Marriott International will now have the opportunity to make representations to the ICO as to the authority's proposed findings and sanction. Under the GDPR 'one stop shop' provisions, the data protection authorities in the EU whose residents have been affected will also have the chance to comment on the ICO's findings.

11.2.4.4 Blocking statutes

Blocking statutes prevent the disclosure of certain documents for the purpose of legal proceedings in a foreign jurisdiction, except pursuant to procedures set out in an international treaty or agreement. Article 1*bis* of the French Blocking Statute provides:

> *[I]t is prohibited for any person to request, to investigate or to communicate in writing, orally or by any other means, documents or information relating to economic, commercial, industrial, financial or technical matters leading to the establishment of proof with a view to foreign administrative or judicial proceedings or as a part of such proceedings.*

There has historically been very little enforcement of the French Blocking Statute – with some companies choosing to ignore it completely.[54] However, as a consequence of the Sapin II law, which was implemented in June 2017, France's financial crime agency (Parquet National Financier (PNF)) has begun to lead cases involving the enforcement of the Blocking Statute, signalling that the French authorities are considering the issues raised by the Blocking Statute in more depth.

The French government is currently considering a report submitted by a French member of parliament in June 2019, which includes recommended reforms to the French Blocking Statute. The report calls for amendments to force foreign authorities to co-operate with French authorities instead of 'systematically' bypassing conventions of international co-operation. The report also calls for a significant increase in penalties for any violations of the French Blocking Statute.[55] The French anti-corruption regulator (Agence Française Anticorruption (AFA)) is responsible for ensuring compliance with the Blocking Statute.

The joint guidelines on the French equivalent of the DPA (*convention judiciaire d'intérêt public* (CJIP)) recently issued by the PNF and AFA indicate the French authorities' willingness to enter into coordinated settlement discussions with foreign enforcement authorities in cases involving multi-jurisdictional misconduct. The new guidelines do not set out any differences in complying with the Blocking Statute when co-operating with foreign enforcement authorities.

54 Despite its very protective wording, the French Blocking Statute has received a very limited application – only one criminal conviction (under Article 1*bis*) has ever been recorded (Cass. Crim, 12 December 2007, n°07-83.228).

55 Raphaël Gauvain, 'Rétablir la souveraineté de la France et de l'Europe et protéger nos enterprises des lois et mesures à portée extraterritoriale', National Assembly report (26 June 2019).

Therefore adherence to the Blocking Statute is expected. However, the guidelines suggest that when the PNF negotiates a joint settlement with other authorities, it may propose that the AFA act as a monitor to prevent a violation.[56]

The French authorities have traditionally taken any derogation from the letter of the law seriously and insist on the use of MLA requests and inter-agency communications. This can leave companies in the unenviable position of being caught between authorities (if the US authorities, for example, expect production directly from the corporate). In such circumstances, agency-to-agency communications should be encouraged. Similarly, Article 271 of the Swiss Criminal Code prohibits a person performing an 'official act' on behalf of a foreign authority on Swiss soil. This can block the collection of evidence located in Switzerland intended for use in proceedings outside the country.

China is another jurisdiction to have enacted laws to block the transfer of information to foreign government authorities in criminal proceedings. On 26 October 2018, China enacted the International Criminal Judicial Assistance (ICJA) law with immediate effect, prohibiting institutions, organisations and individuals within China from providing evidentiary materials and assistance to foreign countries in criminal proceedings (e.g., before seeking to comply with a subpoena from a foreign government authority in a criminal investigation) without approval from the competent Chinese authorities. In accordance with the ICJA law, this legislation is to be applied in a manner that does not harm national sovereignty, security or public interests, giving the Chinese government broad discretion to refuse or block foreign governments' requests for assistance. The ICJA law governs all requests for 'judicial assistance' between China and foreign jurisdictions in relation to international criminal proceedings, including the service of documents, evidence collection, witness testimony, seizure and confiscation of illegal assets, and the transfer of convicted persons.

A decision to refuse to disclose documents or information due to a blocking statute may not be respected by the requesting authority[57] and could affect any co-operation credit available – leaving the company between a rock and a hard place. This demands early and detailed dialogue with the relevant authority alongside expert local counsel who can educate the regulators about the relevant laws and any potential workarounds for production of information.

Bank secrecy 11.2.4.5

Bank secrecy laws prohibit banking officials from releasing confidential information about a customer to third parties outside of financial institutions, unless compelled by law. Sometimes, such a disclosure is criminalised.[58] A bank under investigation may seek to rely on this secrecy. It should also be cautious not to infringe

56 See https://www.agence-francaise-anticorruption.gouv.fr/files/files/Lignes%20directrices%20PNF%20CJIP.pdf.

57 For an English case dealing with the French Blocking Statute, see *Secretary of State for Health v. Servier Laboratories; National Grid Electricity Transmission v. ABB* [2014] WLR 4383.

58 See most famously Article 47 of the Swiss Federal Act on Banks and Savings Banks (1934).

this secrecy inadvertently in providing information to a regulator. Note, though, that a historic deference to the banking secrecy rules of foreign jurisdictions, premised on comity or respect for the acts of foreign governments, may slowly be eroding. Even Switzerland, in recent times, has stripped away a number of its many layers of secrecy through international agreements,[59] and, in our experience, has become, in practice, more willing to co-operate with requests for information.

11.2.4.6 State secrets

Sending data outside a jurisdiction may be contrary to state secrecy laws. Some jurisdictions, such as China, have wide definitions of what amounts to a state secret. The Law of the People's Republic of China on Guarding State Secrets, at Article 8, defines state secrets to include 'secrets in national economic and social development' and 'secrets concerning science and technology'. Similarly, Kazakhstan treats some geological data as a state secret. The consequences of violation can be serious. Article 111 of the Chinese Criminal Law makes violating state secrets a capital crime. In countries such as China, where many companies are state-owned, this is not straightforward. Again, locating expert local counsel is a must.

State secrecy laws may also restrict certain categories of documents to authorised eyes only. This is particularly pertinent for defence companies. Withholding production of such documents will require careful negotiation. Remember that the investigating agency is likely to have authorised persons of its own, who can review the documents. Finding a practical way for these to be produced by external lawyers (where prior authorisation is unlikely) will likely be more difficult and undoubtedly will increase the time it will take to respond to a request for documents and may require the review of documents 'in country' instead of producing the documents to the US authorities. Another potential workaround is production of information through MLATs and memoranda of understanding that allow a company to first produce documents to a local authority and thereby comply with the relevant regulations.

11.2.4.7 Whose rules of privilege apply?

It may not be clear whose rules of privilege apply when a company discloses in one jurisdiction documents created in another. English courts will generally apply English law to the question: theoretically, an unprivileged document in its country of origin could be privileged in England and *vice versa*. In the United States, there is no general rule, although government agencies will generally apply privilege principles broadly, although subject to certain procedural requirements, such as the production of privilege logs.

59 See, e.g., Switzerland's entrance, in October 2013, to the Multilateral Convention on Mutual Administrative Assistance on Tax Matters, and agreement to increase transparency and exchange financial information with approximately 60 other countries.

Companies should also be aware that some countries do not have developed principles of legal privilege and special care is required in creating or sending otherwise privileged documents to such jurisdictions. Likewise, in some jurisdictions privilege does not extend to communications with in-house counsel and the role of internal counsel may be held by someone who is not an attorney, and therefore privilege may not be recognised in connection with their communications.

Further complications come when dealing with international regulatory bodies. In *Akzo Nobel*, for example, the European Court of Justice held that the law of the European Union superseded that of the relevant national jurisdictions; therefore, in competition cases internal counsel's advice will not be privileged – nor will that of external legal advisers who are not EU-qualified lawyers.[60]

Documents obtained through dawn raids, arrest and search 11.3

During a raid (or execution of a search warrant) on corporate premises, it is important to seek to obtain and understand the terms of the warrant. Check simple facts such as the premises' address, the date and relevant powers and authorisations. If appropriate, a company may challenge the scope of the warrant (if it is unduly wide or based on erroneous facts or information). Importantly, the company and its advisers should ensure during the raid that documents outside the terms of the warrant are not seized (unless taken under relevant search and sift powers,[61] or as can be justified under ancillary legislation)[62] and take care both during the raid and afterwards to protect legally privileged materials. In the United States, it is nearly impossible to challenge the scope of a warrant that calls for the immediate search of a specific location. More likely, a company would have to seek to suppress evidence obtained pursuant to a warrant in a later proceeding. There may, however, be opportunities to challenge the scope of a warrant seeking electronically stored information before the data is actually collected and produced. As an example, where a company is asked to execute a warrant on behalf of the government, such as when a service provider is asked to collect electronic information of a third party, there may be additional opportunities for a company to challenge the scope of a subpoena. It is likely that the vast majority of documents obtained during a search will be electronic. It is important to agree to a process with the authorities for dealing with any electronic media that is privileged. In the United

60 *Akzo Nobel Chemicals v. European Commission* (Case C-550/07, European Court of Justice, 14 September 2010). Here, the Court held that internal company communications with in-house lawyers subject to a European Commission investigation were not covered by legal professional privilege, as, for the purposes of such an investigation, an in-house lawyer was not sufficiently independent.

61 For the United Kingdom, see s.50 of the Criminal Justice and Police Act 2001. In the United States, prosecutors will often establish what are referred to as 'taint teams' to review potentially privileged information. Justice Manual § 9-13.420 (Searches of Premises of Subject Attorneys) provides guidance for the review of material seized not only from an attorney's office but also from 'searches of business organizations where such searches involve materials in the possession of individuals serving in the capacity of legal advisor to the organization'.

62 See s.19(5) of the Police and Criminal Evidence Act 1984.

Kingdom, most investigative agencies have developed sophisticated procedures in this area. The SFO's policy and system for dealing with material covered by legal professional privilege (LPP) is explained in its Operational Handbook:

> *When the SFO requires the production of material, or seizes material pursuant to its statutory powers, all material which is potentially protected by LPP must be treated with great care to:*
> - *Minimise the risk that LPP material is seen or seized by an SFO investigator or a lawyer involved in the investigation.*
> - *Ensure that any LPP material which is seized is properly isolated and promptly returned to the owner without having been seen by an SFO investigator or a lawyer involved in the investigation.*
> - *Ensure that any dispute relating to LPP is resolved in advance of the material being seen by an SFO investigator or a lawyer involved in the investigation.*
> - *Ensure that where an SFO investigator or a lawyer involved in the investigation inadvertently sees LPP material, measures are in place to ensure that the investigation and any subsequent prosecution is not adversely affected as a result. Care must always be taken that LPP material is not viewed by the SFO staff involved in the investigation.*[63]

The Operational Handbook then sets out a procedure for dealing specifically with electronic material that may be privileged. Under this procedure, the SFO will first notify the company's lawyers if it believes that IT assets it has seized might contain privileged material (in practice, it is prudent for the company's lawyers to advise the SFO of the potential existence of privileged material at an early stage). A list of search terms should be agreed (including names of lawyers, relevant firms, etc.) to enable the identification and isolation of the material for review by independent counsel. Independent counsel will review the material using search software and return only non-privileged material to the SFO investigative team to examine. It is normally possible to have productive discussions with investigators to determine the relevant search terms that might identify privileged material. It is then possible to make representations on the client's behalf to independent counsel about the extent of privilege. This procedure updates and works alongside the well-established 'blue-bagging' approach used for hard-copy materials that may be privileged, by which authorities will send seized documents that may be

63 Cited in *R (on the application of Colin McKenzie) v. The Director of the Serious Fraud Office* [2016] EWHC 102, at [8] (original emphasis). In this unsuccessful challenge to this procedure, the essential question was whether, as a matter of law, the process for isolating files that may contain legal professional privilege (LPP) material into an electronic folder for review by an independent lawyer must itself be carried out by individuals who are independent of the seizing body. The court held that the procedure set out in the SFO's Handbook for isolating material potentially subject to LPP, for the purpose of making it available to an independent lawyer for review, was lawful.

potentially privileged, sealed in an opaque bag, to the custody of an independent legal adviser (usually a barrister) for review.

The DOJ has used three different procedures for reviewing potentially privileged information, each of which requires a 'neutral' third party to first review potentially privileged data.[64] In certain instances the court may review the data on its own. A court may also appoint a 'special master' to handle the review of privileged information.[65] In other instances, a team of individuals referred to as a 'taint team' may be used to review the files.[66] When a taint team is used, an ethical wall will be placed between the individuals who review the documents and those who are actually participating in the investigation.[67] Importantly, courts have had differing reactions to the use of taint teams and may not always conclude that the procedures implemented to screen materials were sufficient.

Disclosure of results of internal investigation 11.4

In most instances, a company will have to make expansive disclosures regarding its internal investigations to get full co-operation credit. The DOJ has issued guidance in the Justice Manual[68] that explicitly states that companies will have to self-report on both the results of internal investigations and on individual misconduct to receive any co-operation credit.[69] Whether such thorough disclosures are in the best interest of the company is something that will need to be determined in a timely manner.

64 See Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

65 See, e.g., Order Appointing Special Master, *United States v. Cohen*, Dkt No. 30, Case No. 18-mj-3161 (S.D.N.Y. 27 April 2018).

66 Searches of Premises of Subject Attorneys, Justice Manual, § 9-13.420.

67 See, e.g., Order Appointing Special Master, *United States v. Cohen*, Dkt No. 30, Case No. 18-mj-3161 (S.D.N.Y. 27 April 2018); Order, *United States v. Gallego*, Dkt No. 65, Case No. 4:18-cr-01537 (D. Ariz. 6 September 2018).

68 The Value of Cooperation, Justice Manual § 9-28.700; Cooperation: Disclosing the Relevant Facts, Justice Manual § 9-28.720; FCPA Corporate Enforcement Policy, Justice Manual § 9-47.120, available at https://www.justice.gov/criminal-fraud/file/838416/download (full cooperation requires, among other things, prompt disclosure of 'all facts related to involvement in the criminal activity by the company's officers, employees, or agents; and all facts known or that become known to the company regarding potential criminal conduct by all third-party companies (including their officers, employees, or agents').

69 The November 2019 amendments to the FCPA Corporate Enforcement Policy acknowledge that a company may not know all facts relevant to misconduct at the time of a voluntary self-disclosure. The revised policy emphasises that in order to receive cooperation credit, a company should 'make clear that it is making its disclosure based upon a preliminary investigation or assessment of information, but it should nonetheless provide a fulsome disclosure of the relevant facts known to it at the time'. Justice Manual § 9-47.120 at note 1.

11.4.1 Self-reporting of misconduct not yet known to regulators

A company's decision as to whether to self-report is often complicated. There may be opportunities for a company to internally address misconduct without it coming to light. However, it can be very difficult for a company to keep its misdeeds from being disclosed to the relevant authorities. Whistleblower rewards provide incentives for employees to report misconduct. Federal statute provides protections for whistleblowers,[70] and in 2017 the SEC imposed financial penalties on financial institutions that attempt to prohibit employees from seeking those bounties.[71] Disgruntled employees can report corporate misconduct as retaliation, to attempt to prevent prosecution of themselves or simply because they do not feel that the corporate is handling the issue appropriately via its internal process. In the United Kingdom, broadly speaking, those working in the field of financial services are subject to suspicious activity reporting obligations. This means that banks, accountants and transactional lawyers must make reports to the authorities of suspicions of money laundering (including acquiring assets which may be tainted by fraud or corruption). A failure to make a report is a criminal offence – as is tipping off the subject of the report (which in some instances may be the individual's own client). Investigative journalism and non-governmental organisations also continue to be important sources of information for regulators – as the 'Panama Papers' scandal illustrated.[72]

A failure to self-report misconduct before it becomes otherwise known to the authorities can have a significant impact on the resolution of the corporate investigation. The Justice Manual (which governs the conduct of Assistant US Attorneys during the course of civil and criminal investigations, including FCPA investigations) provides that:

> *Even in the absence of a formal program, prosecutors may consider a corporation's timely and voluntary disclosure, both as an independent factor and in evaluating the company's overall cooperation and the adequacy of the corporation's compliance program and its management's commitment to the compliance program. However, prosecution may be appropriate notwithstanding a corporation's voluntary disclosure. Such a determination should be based on a consideration of all the factors set forth in these Principles.*[73]

70 See Section 922(h) of the Dodd-Frank Wall Street Reform and Consumer Protection Act, 15 U.S.C.A. § 78u-6(h)(1)(A) (2010).

71 See https://www.sec.gov/news/pressrelease/2017-14.html (announcing penalty imposed on BlackRock Inc., based on its inclusion of language in separation agreements requiring former employees to waive any incentives they might be entitled to for reporting the company's misconduct); https://www.sec.gov/news/pressrelease/2017-24.html (announcing penalty imposed on HomeStreet Inc. for improper accounting and steps taken to impede whistleblowers).

72 The Panama Papers are available through the International Consortium of Investigative Journalists' dedicated website, at https://panamapapers.icij.org/.

73 Justice Manual § 9-28.900 (internal citations omitted).

As we have already noted, under the FCPA Corporate Enforcement Policy, receiving full credit for voluntary self-disclosure requires, among other things, prompt disclosure of 'all relevant facts known to it at the time of the disclosure, including as to any individuals substantially involved in or responsible for the misconduct at issue'.[74] The recent amendments to the Corporate Enforcement Policy clarify that a company does not need to disclose information regarding *all* individuals that may have been involved in wrongdoing. Instead, it is required to disclose 'any individuals *substantially* involved in or responsible for the *misconduct* at issue'.[75] Moreover, the company will have to disclose 'on a timely basis . . . all facts relevant to the wrongdoing at issue, including: all relevant facts gathered during a company's independent investigation; attribution of facts to specific sources where such attribution does not violate the attorney–client privilege, rather than a general narrative of the facts; timely updates on a company's internal investigation, including but not limited to rolling disclosures of information'.[76]

The Deferred Prosecution Agreements Code of Practice (the DPA Code) issued by the SFO and the Crown Prosecution Service[77] indicates that, to be eligible for a DPA, a company will likely have to report voluntarily any misconduct within a reasonable time of becoming aware of it – and prior to it becoming known to the authorities. In fact, in a number of the five DPA cases,[78] the companies self-reported their misconduct to the SFO in circumstances where the SFO had no prior knowledge of the misconduct and, in all likelihood, would not have learnt about the misconduct if the company had not self-reported.

But, in the *Rolls-Royce* case, which was concluded by a DPA in January 2017, the company did not self-report to the SFO the conduct that led to the SFO's investigation. Instead, the SFO became aware of the need for an investigation through internet postings by a whistleblower. The fact that Rolls-Royce did not self-report weighed against the SFO offering a DPA; yet, Rolls-Royce chose to co-operate fully with the investigation after the SFO approached the company, and undertook its own internal investigation (in close consultation with the

74 Justice Manual § 9-47.120(3)(a). The Justice Manual has recently been revised to acknowledge that a company may not necessarily be in possession of all of the relevant information at the time of its initial disclosures. In such circumstances, a disclosing company should make clear that it is making an initial disclosure based on its preliminary investigation or assessment of information. Justice Manual § 9-47.120 at note 1.

75 Justice Manual § 9-47.120(3)(a) (emphasis added). This change makes the disclosure requirements consistent with prior guidance issued by the US Attorney's Office and other provisions of the Justice Manual.

76 Justice Manual § 9-47.120 (3)(a).

77 DPA Code, para. 2.8.2(i).

78 *SFO v. Standard Bank plc* (Case No. U20150854) [2016] Lloyd's Rep FC 102 and *SFO v. XYZ Ltd* (Case No. U20150856) [2016] 7 WLUK 220; [2016] Lloyd's Rep FC 509. In the case of *SFO v. Tesco Stores Limited* [2019] Lloyd's Rep FC 283, Tesco identified issues in its financial statements, and referred itself to enforcement authorities after revealing that revenues had been incorrectly recorded as profits and made an announcement to the market. In *SFO v. Serco Geografix Ltd.* (Case No. U20190413) [2019] 7 WLUK 45, the company disclosed material discovered after an initial SFO investigation found no evidence of any dishonest or fraudulent activity.

SFO). In total, Rolls-Royce collected over 30 million documents and subjected them to electronic document review as part of this investigation. One of the main features of Rolls-Royce's co-operation was that it provided all materials requested by the SFO voluntarily, without the SFO having to compel it to provide information. Rolls-Royce also chose not to perform any legal professional privilege review over the documents (instead allowing independent counsel to resolve issues of privilege) and worked with the SFO as the SFO used sophisticated artificial intelligence searches to interrogate the data. This process led to the SFO uncovering information that may not have otherwise come to its attention. Ultimately, SFO counsel described the extent of Rolls-Royce's co-operation with the investigation as 'extraordinary'.

While the decision to provide documents voluntarily to the SFO was one of a number of measures taken by Rolls-Royce to demonstrate its co-operation with the investigation, this decision was of fundamental importance to the court when deciding to approve the DPA. Rolls-Royce's voluntary disclosure of investigation documents therefore mitigated its failure to voluntarily disclose misconduct.

11.4.2 Production of reports of investigation

To obtain co-operation credit, prosecuting and government agencies require that companies provide the complete factual findings of an internal investigation, including relevant source documents. The Justice Manual recognises 'the sort of cooperation that is most valuable to resolving allegations of misconduct by a corporation and its officers, directors, employees, or agents is disclosure of the relevant facts concerning such misconduct'.[79]

Similarly, the DPA Code provides that co-operation will include 'providing a report in respect of any internal investigation including source documents'.[80]

Careful consideration should be given to the manner of disclosure of information. In the United States, the consideration for credit is that the relevant facts are disclosed. The format of the disclosure is irrelevant. The Justice Manual makes it clear that a company does not have to waive privilege to receive co-operation credit.[81] If a company chooses not to waive relevant privileges, it is unlikely to be able to share the investigative reports prepared by counsel conducting the investigation. Instead, it will have to carefully craft presentations that disclose only non-privileged facts. Preparation of such reports can be time-consuming and costly. Further, in preparing any written presentation materials, the company will have to ensure that neither the mental impressions nor advice of counsel are included. Because there can be no claim that the materials are privileged, a company should also expect that they will have to produce presentation materials in any related civil litigation.

79 See Justice Manual § 9-28.720 (Cooperation: Disclosing the Relevant Facts).

80 DPA Code, para. 2.8.2(i).

81 See Justice Manual § 9-28.720. The FCPA Corporate Enforcement Policy refers to Justice Manual § 9-28.720 and states that a company will not have to waive privilege to receive full co-operation credit.

In the United Kingdom, there is currently much debate over the production of the first accounts of witnesses, which may have been taken by investigating attorneys. The SFO's preference is that these are taken so that legal privilege does not apply. It also indicates that it does not consider all privilege claims over interview materials to be made out under English law and until the Court of Appeal's decision in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* (*ENRC*),[82] was actively challenging such assertions. Where a valid claim for privilege exists, co-operation credit will be given for the disclosure of interview memoranda. A failure to disclose will be considered co-operation neutral. As Alun Milford, then SFO General Counsel, has previously said: 'If a company's assertion of privilege is well-made out, then we will not hold that against the company: to do otherwise would be inconsistent with the substantive protection privilege offers.'[83] In two of the UK cases in which the court has approved DPAs, the company made oral disclosure only of the content of witness interviews.[84] However, Rolls-Royce chose to provide the interview memoranda to the SFO – even though it considered the memoranda to be privileged – on the basis of a limited waiver of privilege. This was another way Rolls-Royce used the voluntary disclosure of documents to counterbalance its failure to voluntarily disclose the misconduct. Other materials voluntarily provided to the SFO by Rolls-Royce included regular reports on the findings of the internal investigations; unfiltered access to the 'digital repositories or email containers' for over 100 past and present employees; general access to hard-copy documents at Rolls-Royce; and key documents identified by the internal investigations. Finally, Rolls-Royce held off interviewing potential witnesses until the SFO had the chance to do so.[85] How a company makes its employees available to investigating authorities is important, and this chapter will now turn to this issue.

The SFO has recently affirmed its position on witness accounts and privilege as part of the Corporate Co-operation Guidance, which confirms that a company's failure to waive privilege means that it will not attain the corresponding factor against prosecution in the DPA Code, but that the SFO will not penalise the company in this regard. The Corporate Co-operation Guidance suggests that

82 [2018] EWCA Civ 2006.

83 Alun Milford, then SFO General Counsel, 'Speech to compliance professionals' (given to the European Compliance and Ethics Institute, Prague, 29 March 2016.)

84 See, e.g., *SFO v. XYZ* (Preliminary Judgment) Crown Court, Southwark, U20150856 (20 April 2016): '[C]o-operation includes identifying relevant witnesses, disclosing their accounts and the documents shown to them: see para. 2.8.2(i) of the DPA Code of Practice. Where practicable it will involve making witnesses available for interview when requested. In that regard, XYZ provided oral summaries of first accounts of interviewees, facilitated the interview of current employees, and provided timely and complete responses to requests for information and material, save for those subject to a proper claim of legal professional privilege.'

85 In securing DPAs, both Tesco and Serco received co-operation credit for refraining from interviewing witnesses at the request of the FCA/SFO. See *SFO v. Tesco Stores Limited* (Case No. U20170287) [2019] Lloyd's Rep FC 283 and *SFO v. Serco Geografix Ltd.* (Case No. U20190413) [2019] 7 WLUK 45.

while an organisation will not get the full co-operation credit potentially available in these circumstances, the SFO will not automatically refuse a DPA if it can demonstrate other co-operative factors pointing against a public interest in prosecuting the company, in accordance with the DPA Code.[86]

11.4.3 Identification of witnesses to authorities

In connection with its initial assessments of whether to co-operate with authorities, companies will have to consider the implications of disclosing information about key employees. As noted above, US and UK authorities have indicated that co-operation will require disclosure of facts relevant to the misconduct of individual employees.

In the United States, authorities have made clear that obtaining facts relevant to individual prosecutions is a top priority. The Justice Manual provides that '[i]n order for a company to receive any consideration for cooperation under this section, the company must identify all individuals substantially involved in or responsible for the misconduct at issue, regardless of their position, status or seniority, and provide to the Department all relevant facts relating to that misconduct'.[87]

Additionally, the 'unequivocal co-operation' necessary to be eligible for a DPA in the United Kingdom includes identifying relevant witnesses, disclosing their accounts of the alleged misconduct and any documents shown to them and, where practicable, making those witnesses available for interviews by investigators[88] – together with ongoing co-operation with the authorities.

When seeking a DPA, a corporate should consider liaising closely with the SFO, which may wish to undertake witness interviews, or interviews under caution,[89] with individuals prior to corporate counsel doing so. The Corporate Co-operation Guidance confirms that the SFO will expect organisations to identify individuals responsible for the suspected wrongdoing (and support the SFO's disclosure obligations in its prosecution of individuals) and potential witnesses, and that co-operating companies should consult with the SFO before interviewing potential witnesses or suspects, taking HR actions or other overt steps. Once the individuals have been identified to the government or prosecuting authorities it may be difficult, if not impossible, for those individuals to continue working

86 SFO Operational Handbook, Corporate Co-operation Guidance, p. 5.

87 The Value of Cooperation, Justice Manual § 9-28.700; see also Cooperation: Disclosing the Relevant Facts, Justice Manual § 9-28.720. The November 2019 amendments to the FCPA Corporate Enforcement Policy made the various provisions regarding disclosures of individuals involved in wrongdoing more consistent.

88 DPA Code, para. 2.8.2(i).

89 Where a defendant in the United Kingdom is suspected of committing a criminal offence, and is questioned in relation to it (whether while under arrest or voluntarily), the questioner must administer a 'caution' for any evidence provided in the interview to be admissible in subsequent proceedings. The caution sets out interviewees' rights and how any evidence they provide at interview may be used against them in a trial. An organisation or company can be interviewed under caution through a nominated spokesperson, who will attend the interview to answer questions on its behalf.

for the company. A company may feel pressure to terminate the employee or place that individual on leave, which could have a significant impact on the operations of a business unit. Even if the company does not terminate an employee under investigation, targets of a government investigation are likely to engage their own counsel who may advise the employee to stop co-operating with its employer – leading to a 'walk or talk' decision. Depending on the nature of any employment agreement, a company may have to advance the individual the fees and costs associated with individual representation. Also, since 2004, the United Kingdom has imposed an extensive Code of Practice for Disciplinary and Grievance Procedures on employers, which sets out standards of procedural fairness that a UK employer should comply with if it takes action that will detrimentally affect an employee's employment.[90]

See Chapters 13 and 14 on employee rights

Privilege considerations 11.5

In the United States, certain portions of internal investigations are protected by the attorney–client privilege and the work-product doctrine, and courts routinely uphold those privileges.[91] This can be true even where the purpose of an investigation is to ensure regulatory compliance, or where non-lawyers are involved in key parts of the investigation.[92]

Generally, the attorney–client privilege entitles a party to withhold from production (1) communications, (2) with an attorney, his or her subordinate or agent, (3) made in confidence, (4) for the primary purpose of securing an opinion of law, legal services or assistance in a legal proceeding. It applies to corporations as well as individuals, and therefore protects communications between corporate employees and a corporation's in-house and external legal counsel on matters within the scope of the employees' corporate responsibilities. Communications between non-legal corporate employees can also be privileged where an attorney neither authors nor receives the communication, if the communication contains or refers to previously transmitted legal advice or identifies specific legal advice that the non-attorneys will seek from attorneys in the near future. Additionally, the work-product doctrine protects documents and tangible things, otherwise discoverable, prepared in anticipation of litigation and in connection with a threatened or pending government investigation. The doctrine can apply to documents prepared by both attorneys and non-attorneys. Attorney notes, research, and

90 ACAS 'Code of practice on disciplinary and grievance procedures' (2015) available at https://www.acas.org.uk/media/1047/Acas-Code-of-Practice-on-Discipline-and-Grievance/pdf/11287_CoP1_Disciplinary_Procedures_v1__Accessible.pdf.

91 See *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754 (D.C. Cir. 2014); *Cicel (Beijing) Sci. & Tech. Co. v. Misonix, Inc.*, No. 17CV1642, 2019 WL 1574806 (E.D.N.Y. Apr. 11, 2019); *In re Gen. Motors LLC Ignition Switch Litig.*, 80 F. Supp. 3d 521, 530 (S.D.N.Y. 2015).

92 *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 760 (D.C. Cir. 2014), at 760. ('In the context of an organization's internal investigation, if one of the significant purposes of the internal investigation was to obtain or provide legal advice, the privilege will apply. That is true regardless of whether an internal investigation was conducted pursuant to a company compliance programme required by statute or regulation, or was otherwise conducted pursuant to company policy.') (Citation omitted.)

compilations of background materials, memoranda, investigative reports, witness statements; and materials prepared by non-legal personnel such as investigators are examples of the types of documents that may be protected. Work-product containing an attorney's mental impressions is referred to as 'opinion' work-product and is afforded greater protection than other 'ordinary' work-product.

In the United Kingdom, privilege attaches to (1) confidential communications between a lawyer and his or her client for the purpose of seeking and receiving legal advice in a relevant legal context, including factual reporting (legal advice privilege), and (2) confidential communications between a lawyer and his or her client and/or a third party, or between a client and a third party, provided that such communications have been created for the dominant purpose of obtaining legal advice, evidence or information in preparation for actual litigation, or litigation that is 'reasonably in prospect' (litigation privilege). English case law has traditionally called into question the availability of litigation privilege for documents created during a regulatory investigation, as an investigation alone lacks the adversarial character of litigation. In the recent *ENRC*[93] decision, the Court of Appeal looked at the issue of when a corporate might reasonably contemplate prosecution (and therefore the necessary 'litigation') in the context of a self-reporting process, commenting as follows:

> *[W]e are not sure that every SFO manifestation of concern would properly be regarded as adversarial litigation, but when the SFO specifically makes clear to the company the prospect of its criminal prosecution . . . and legal advisers are engaged to deal with that situation, as in the present case, there is a clear ground for contending that criminal prosecution is in reasonable contemplation.*[94]

But, the Court went on to say that no particular action in the course of engagement with a regulator will allow a company to say that at a particular date it contemplated a criminal prosecution and privilege crystallised. Every case will turn on its own facts, and the evidence will be assessed in the round.

The corporate must also have created the documents for the dominant purpose of the contemplated litigation. In *ENRC*, even where ENRC might have created documents for the dominant purpose of merely investigating 'the facts to see what had happened and deal with compliance and governance',[95] the Court said this:

> *Although a reputable company will wish to ensure high ethical standards in the conduct of its business for its own sake, it is undeniable that the 'stick' used to enforce appropriate standards is the criminal law and, in some measure, the civil law also. Thus, where there is a clear threat of a criminal investigation, even at one remove from the specific risks posed by the SFO should it start an investigation, the reason for the investigation of whistle-blower allegations*

93 [2018] EWCA Civ 2006.

94 At [96].

95 At [108].

> *must be brought into the zone where the dominant purpose may be to prevent or deal with litigation.*[96]

So, litigation privilege may well cover a significant proportion of documents created in the course of an internal investigation into possible criminal activity after the regulator has made clear there is a prospect of prosecution. Again, though, why the corporate created particular documents is important. If a corporate creates documents specifically to disclose to the regulator, then it seems unlikely that a claim to litigation privilege against that same regulator will succeed, at least in relation to the final versions of these documents.

The Court of Appeal also discussed the policy behind applying litigation privilege in this area:

> *It is, however, obviously in the public interest that companies should be prepared to investigate allegations from whistle blowers or investigative journalists, prior to going to a prosecutor such as the SFO, without losing the benefit of legal professional privilege for the work product and consequences of their investigation. . . . The remedy for the SFO is not to allow prevarication and delay . . . to prevent a timeous investigation, when it becomes clear that the company is not wholeheartedly reporting its own conduct and making appropriate waivers of privilege.*[97]

It went on to make clear that determining the extent of co-operation by a company (in an analysis of whether a DPA was in the public interest) included determining 'whether the company was willing to waive any privilege attaching to documents produced during internal investigations, so that it could share those documents with the SFO'.[98] But, as noted above, past practice in both the United Kingdom and the United States suggests that a corporate does not need to waive privilege over all its investigation documents to receive co-operation credit.

On 2 October 2018, the SFO announced that it would not appeal the *ENRC* decision further to the Supreme Court.[99]

In presenting the underlying facts of an internal investigation, a company must be mindful of the inherent risk that such a presentation will be deemed a privilege waiver in any subsequent proceedings. If a disclosure of privileged information to a federal office or agency is deemed intentional, the privilege will be waived in any federal or state proceeding.[100] However, if a disclosure of privileged information is unintentional, it will not create a broad waiver so long as the holder of the privilege

96 At [109].

97 At [116].

98 At [117].

99 Kirstin Ridley, 'UK fraud office backs down in ENRC privilege battle', *Reuters* (2 October 2018), available at https://uk.reuters.com/article/uk-britain-enrc-sfo/uk-fraud-office-backs-down-in-enrc-privilege-battle-idUKKCN1MC1N0.

100 See Fed. R. Evid. 502(a).

took steps to prevent the disclosure and then promptly took reasonable steps to seek return of any inadvertently disclosed information.[101] Accordingly, if a company decides that it does not intend to waive privilege, it should devise reasonable steps that highlight the company's decision not to waive privilege, including providing written notice of the intention not to produce privileged materials in any letter or other correspondence that accompanies a document production. Courts in England and Wales have held that a company can share the contents of a privileged communication with a regulator or other third party, keeping the privilege intact, so long as this desire is made clear, the disclosure is confidential and the communication is not proliferated widely.[102]

See Chapters 35 and 36 on privilege

The SFO has clarified its position on privilege considerations as part of the Corporate Co-operation Guidance, confirming that if an organisation decides to assert legal privilege over relevant materials (such as first accounts, internal investigation interviews or other documents), the SFO may challenge the privilege assertion where it considers it necessary or appropriate to do so. The Corporate Co-operation Guidance also includes an additional step for companies, by requiring organisations claiming privilege over materials to provide certification by independent counsel that the material is privileged. This is a departure from current practice and will serve as an additional cost for organisations under investigation.

11.6 Protecting confidential information

Companies producing information to the government should take steps to protect the confidentiality of that information. Although information produced in response to a grand jury subpoena must be kept confidential,[103] in the absence of a formal request, documents and testimony provided to the DOJ, SEC or other government authority can be shared with others. In many instances, documents under the control of a government agency can be subject to requests made pursuant to the Freedom of Information Act (FOIA).[104] Further, documents typically shielded from disclosure by the FOIA and other regulations are not exempt from production to the United States Congress, which can, in turn, make the information public.

The procedures necessary to shield confidential information from disclosure can be quite complex. Each regulatory body has its own procedures for seeking confidential treatment of information. The SEC, for example, requires that each page of a document containing confidential information be stamped with a specific legend and that a request for confidential treatment go to the individual receiving the documents and the Office of Freedom of Information and Privacy Act Operations.[105] Many states have their own versions of the FOIA governing the treatment of information provided to, among others, state attorneys

101 See Fed. R. Evid. 502(b).
102 See *Gotha City v. Sotheby's* [1998] 1 WLR 114 (CA).
103 Fed. R. Crim. Pro. 6(e).
104 5 U.S.C. § 552.
105 17 C.F.R. § 200.83

general.[106] Further, while some congressional committees may implement their own procedures for seeking confidential treatment of information, an entity producing documents will have to consider what regulations apply to the information sought and whether the specific regulations prohibit disclosure in response to the request.

In the United Kingdom, the High Court confronted these issues in *Standard Life Assurance v. Topland Col*.[107] The SFO had disclosed information it had obtained through its section 2 powers to a Standard Life employee that it wished to interview. The SFO later discontinued the related investigation. Standard Life then used some of this information as part of civil proceedings against Topland. The court noted that the SFO was not entitled to disclose any material obtained by it during an investigation except for the purpose of its investigation (which was the original purpose of the disclosure in this case). A person who wished to prevent disclosure of genuinely confidential information, either by the SFO or by a person it had disclosed documents to, would need to rely on judicial review proceedings or seek an injunction to prevent a breach of confidence. This suggests that, to avoid relying on these indirect remedies, a company should agree with the SFO before disclosure how the SFO might control the further dissemination of confidential or sensitive documents. Safeguards may include the SFO returning the documents following a short time or notifying a disclosing party before the SFO intended to disseminate documents further. On the other hand, a company may also wish to construct potential safeguards around material produced to it during DPA negotiations and that may otherwise be discoverable in subsequent civil proceedings against it.

Concluding remarks 11.7

Companies have an incentive to co-operate with a government investigation, especially if co-operation credit does not necessarily require self-reporting of the misconduct. But self-reporting will assist companies alongside the voluntary provision of relevant materials. The additional advantages of co-operation – control of the investigation process, orderly production of materials and managing press intrusion – are likely to be great when weighed against the disruption and publicity of formal actions including raids, arrests and prosecutions. In cross-border investigations, companies will need to devise due process safeguards to protect the rights of individuals and respect local law requirements. Ensuring local law specialists are instructed to work as part of a multidisciplinary team will be key.

106 See, e.g., New York Freedom of Information Law, Public Officer's Law §§ 84 to 90.
107 *Standard Life Assurance Ltd v. Topland Col* (Rev 1) [2011] 1 WLR 2162.

12

Production of Information to the Authorities: The In-house Perspective

Femi Thomas and Tapan Debnath[1]

12.1 Introduction

Although less common for small and medium-sized enterprises, it is not unusual for large, particularly multinational, companies to find themselves weighing whether to voluntarily disclose information, or what to do when compelled to disclose information to law enforcement or regulatory authorities. The variables to consider are many and nuanced. They include, without limitation, the potential impact on customers and the business, the nature and pervasiveness of the wrongdoing, and whether mandatory reporting obligations arise. This chapter considers some of the key legal and practical considerations implicated when a company produces information to the authorities.

12.2 Initial considerations

The company should as early as possible seek to establish:

- Its status in the inquiry – is it a suspect or witness? This is not always communicated or readily discernible because the authority, itself, might not have decided either way, or might not wish its view to be known in the early stages of an investigation. There may, however, be some clue in how the authority has gone about requesting or otherwise obtaining the information. For instance, in the United Kingdom, a dawn raid by the Serious Fraud Office (SFO) on company premises implies that the SFO, and the courts, have reasonable grounds to believe, based on some assessment of facts, that it is impracticable

1 Femi Thomas is vice president and global head of business integrity at Nokia Corporation and Tapan Debnath is senior legal counsel in Nokia Corporation's ethics and compliance department and compliance lead for Nokia Enterprise Business Group. The views expressed are the authors' (or as otherwise attributed) and do not represent the views of Nokia Corporation.

to use less intrusive production order powers or doing so creates a risk of destruction of evidence. As such, unannounced raids tend to indicate, though not conclusively, that the company is a suspect.[2]

- Are any of the company's employees suspects, and do they pose any ongoing risks to the business?[3] When employees are suspects, a company should ensure that data collection and any internal investigation is conducted without tipping off the implicated employees or 'trampling over the crime scene', while adhering to local data protection and labour law.
- Which authority is making the request, and is the request reasonable? Some authorities are more aggressive than others; this is worth factoring in when setting the response strategy. Equally important is determining whether there are multiple authorities involved. Requests from less familiar jurisdictions, where the independence of prosecutors and the judiciary might be less assured, pose additional questions: Is there a political or monetary motivation? Are employees at risk of arrest and imprisonment without adequate due process? And what are the rules of corporate liability, if any? A request for information should be carefully reviewed to ensure that it appears reasonable in terms of scope and the basis for the request, and should state the power under which the request was made.

Data collection and review 12.3

The company will at an early stage start to think about whether it has the responsive data and the appropriate process for preserving and collecting it. Data from digital devices to be produced to the authorities should be safeguarded from deletion or destruction and then collected in a forensically sound way. At a high level, this means that the collection is carried out by skilled persons who can retrieve and preserve whole images of various types of devices in a manner that is repeatable with consistent results, and that all steps taken are recorded and auditable. It is vital to capture all relevant material, and having a systematic and methodical approach will help. The investigation support team should include someone with detailed knowledge of the company's IT systems and structure and will, preferably, be experienced in data extractions.

A company is also likely to want to understand for itself what the collected data reveals. The data review is invariably the most time-consuming and costly part of the production exercise. It is therefore imperative to try to agree realistic deadlines with the authorities at the outset and to communicate promptly if any slippage is anticipated. Most authorities will want a written record, usually in the

2 On 6 August 2019, the SFO published its long-awaited Corporate Co-operation Guidance. At the end of the Guidance, a short passage explains that it may be necessary for the SFO to exercise powers of compulsion to obtain material from a co-operating company. This re-enforces that how the authority seeks material (whether by production order or dawn raid) can be illustrative only of the company's status in the investigation and should not be taken as conclusive.

3 While change of company personnel (and culture) is a desirable outcome in most cases involving serious wrongdoing, it will probably need to be considered after a thorough review of the issues.

form of witness statements, of the methodology used in the data collection and imaging, the process and rationale behind any filtering of the data, and how the review was conducted and the instructions given to the reviewers. This point is stated explicitly in the Corporate Co-operation Guidance published by the SFO on 6 August 2019 under the heading 'Preserving and providing material'. The SFO Guidance emphasises the need to have an audit trail of the acquisition and handling of digital material and to take all steps to maintain the integrity of systems hosting such material over the life of an SFO investigation, which can run for many years.

A corporate can manage the costs incurred in a data collection and production exercise by: having an established panel of specialist law firms, which should yield discounted rates, but maintaining flexibility to go off-panel as individual case needs dictate; outsourcing the data collection and document review to professional service providers or even doing it in-house[4] if there is the requisite capability, instead of the law firm doing it; ensuring that the document review is as focused as possible through appropriate filtering and, possibly, use of AI technology; setting a budget at the outset and sticking to it unless extensions are approved; and monitoring costs on a monthly basis to ensure the exercise remains within budget.

12.4 Principal concerns for corporates contemplating production

There are numerous, often competing, concerns when a company produces documents to the authorities. One obvious but important concern is the impact that the disclosed material might have on (1) the authority's investigation, or even pre-investigation, and (2) the company's status with the authority. Another concern is to identify and then to protect any intellectual property, trade secrets or proprietary information, or commercially sensitive information that might be contained in, or decipherable from, the material to be disclosed. This concern will accentuate when the company is co-operating with several international and domestic authorities, or where multiple authorities have taken, or could take, an interest. The disclosed material could end up being shared between the various authorities, which could result in the limitations on use that the disclosed material can be put to in one jurisdiction not applying in another. As a result, the disclosing party cannot necessarily ensure that the limitations on use – which applied in the jurisdiction in which the material had been disclosed – will be enforced in a separate jurisdiction in which the material is now available.[5]

4 Some companies have an in-sourced legal support function that handles, for example, initial review of contract terms, which can, with some training and guidance, be used to do the first document review in an internal investigation.

5 In *United States v. Allen*, 864 F.3d 63 (2d Cir. 2017), the US Court of Appeal overturned the convictions and indictments of two LIBOR traders because, among other things, the testimony given by the defendants to the UK Financial Conduct Authority [FCA] under compulsion was used against them in their US criminal trial, which was held to be an infringement of the defendants' Fifth Amendment rights. This is an example of information given in one jurisdiction (the United Kingdom), in which there were statutory limitations on use of the information, being used without limitation, initially at least, by another (the United States).

Special care must be taken at the start and throughout the investigation to have clear records of who is authorised on behalf of the company to instruct and receive advice from external lawyers, and is therefore the client. The purpose of any internal investigation is important also and should be recorded. Is the purpose to obtain legal advice on the company's position in relation to a law enforcement or regulatory authority's interest? Is it to gather information to disclose to the authorities? Or is it to do with actual or contemplated litigation, or a combination of reasons?

At the time of writing the previous edition of this chapter, the England and Wales High Court in *SFO v. ENRC*[6] had ruled that a criminal investigation by the SFO does not necessarily equate to adversarial litigation being in reasonable contemplation, which is of course the test for litigation privilege to be applicable.[7] This made the applicability of legal privilege in internal investigations in the United Kingdom, when the authorities were in an investigatory and not in a prosecution phase, quite difficult and widened the transatlantic divide in the approach to legal privilege. However, in September 2018, the Court of Appeal overturned the High Court's ruling and lowered the bar for legal privilege to be available.[8] Although the key question of whether adversarial litigation is in reasonable contemplation is very fact-specific, it will be a little less difficult for corporates to successfully argue that litigation privilege applies to certain parts of its internal investigation, including over employee and third-party interviews and material generated by forensic accountants.

While the question of who is the 'client' remains narrowly construed, namely those who have been authorised by the company to instruct and receive advice from lawyers, the Court of Appeal in *SFO v. ENRC* expressed a non-binding view that the law in this area could be reviewed and updated. For now, it remains more difficult to apply legal advice privilege to the fact-gathering part of an internal investigation.

A company will also be keen to restrict the ability of third parties to use the information disclosed to the authorities in civil proceedings against the company. Such restrictions could be imposed during the course of negotiations or discussions aimed at resolving, avoiding or reducing the scope of litigation by making clear at the time of production that the information is confidential and, when dealing with UK authorities, stated to be provided on a limited waiver of legal privilege or without-prejudice privilege basis.[9] A company contemplating this approach should

6 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2017] EWHC 1017 (QB), para. 159. The Chancellor of the High Court ruled in *Bilta (UK) Ltd v. Royal Bank of Scotland Plc & Anor* [2017] EWHC 3535 that, in the present case, documents created in an internal regulatory investigation after a 'watershed moment' of HMRC writing to allege tax fraud were covered by legal professional privilege.

7 *Three Rivers District Council and others v. Governor and Company of the Bank of England (No. 6)* [2005] 1 AC 610, HL, para. 53 (*per* Lord Rogers).

8 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2018] EWHC Civ 2006.

9 *Property Alliance Group Ltd v. Royal Bank of Scotland plc* [2015] EWHC 1557 (Ch) without prejudice privilege applied to negotiations with the FCA with a view to arriving at a settlement.

keep in mind that it loses control over material that has been disclosed to authorities. The material might, for example, via court orders for disclosure, end up in the hands of litigants, regardless of attempts to prevent it. Second, the attempt to make the disclosure of material without prejudice to privilege could clash with the authority's expectation of a co-operating entity and negatively affect the chances of non-prosecution. This is particularly the case in view of the 2018 judicial review in which the court criticised the SFO and re-emphasised the SFO's obligation to proactively seek to obtain material that might help the case of individual defendants or undermine the prosecution's case, even if that means testing and challenging a company's assertion of privilege over the product of an internal investigation.[10]

Federal courts in the United States are, however, reluctant to recognise selected waivers of privilege in relation to documents produced as part of an investigation or prosecution.[11] The information may lose the protection of privilege and be subject to discovery by other parties.

See Chapter 36 on privilege

Adherence to data protection principles is another important concern, especially when the information is being provided voluntarily and there is not the protection given by a document production order or subpoena, which usually overrides any local data protection rules. Since 25 May 2018, Article 48 of the EU General Data Protection Regulation (GDPR) has restricted the ability of companies to transfer information out of the European Union in order to respond to orders or requests of foreign courts or authorities. Under this Article, personal data can only be transferred outside the European Union to respond to law enforcement or regulatory subpoenas or production orders, or court orders for disclosure, through the mutual legal assistance treaty route or other provisions of the GDPR. As the application of Article 48 is yet to be examined by the courts, it is unclear whether voluntary disclosure to the authorities is caught by the Article.[12]

12.5 Obtaining material from employees

There will often be a wide pool of employees, a few of whom might be 'suspects' or 'targets', who hold relevant information. It is important to first identify which, if any, of those employees should be notified of the data collection, bearing in mind the SFO cautioning against putting employees on notice and its desire to have the data collection undertaken with minimal risk of interference.[13] The Corporate Co-operation Guidance states that the SFO should be consulted before interviewing employees (or taking any HR action). When collecting data from

---

The without prejudice rule applies to exclude negotiations genuinely aimed at settlement from being given in evidence.

10 See *R (on the application of AL) v. Serious Fraud Office* [2018] EWHC 856.

11 See *In Re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289 (6th Cir. 2002).

12 See, for example, David J Kessler et al., 'The Potential Impact of Article 48 of the The Sedona Conference Journal, volume 17, 2016, No. 2 on Cross Border Discovery From the United States' in The Sedona Conference Journal, Volume 17, 2016, No. 2.

13 Speech by Alun Milford, SFO General Counsel, Annual Employed Bar Conference, 26 March 2014, available at https://www.sfo.gov.uk/2014/03/26/corporate-criminal-liability-deferred-prosecution-agreements/.

employees, the corporation should be mindful of local laws and the company's policies on data collection, as well the potential need to give notice or obtain consent from the employee. The key is to weigh any risk of relevant information being destroyed, and displeasing the requesting authority, if notice of the data collection is given to employees against any specific local law requirements and internal data collection policies.

It is common for employees to have personal material on work devices. If there are no reasonable grounds to believe that giving notice of a data collection exercise to an employee creates a risk that data will be destroyed, the employee could be instructed to separate personal material from work material before the device is copied. The personal material would then be safe from inadvertent disclosure to the authorities. If this separation of personal data is not possible because, for instance, the collection needs to be covert, then filtering and review before disclosure, if appropriate, should provide adequate safeguards against personal data being handed over.

A less common problem is where work material has been stored on personal devices. If that same material also exists on a work device or on the company's servers, it can be collected from there rather than from the employee's personal device. Clearly, it is not possible for a company to covertly extract data from an employee's personal device but it may be possible to do so with the employee's express consent. Such situations should be catered for in the contract of employment and the company's internal policies.

As a best practice, companies should guard against this thorny issue of commingling of personal and business information by instituting appropriately tailored policies. It may not, however, be reasonable to expect that a company device will never be used for some personal purposes but companies should provide written limitations on the kinds of use that are acceptable and permitted. In any event, the transfer of business data through personal devices or email accounts should always be prohibited.

Material held overseas 12.6

Because of the global nature of business, information that is required by a law enforcement or regulatory authority might be held by the company's overseas subsidiaries – and in multiple locations at that.

When a company seeks to provide information voluntarily, it should assess whether this would expose it to potential claims of breaching the confidentiality or data protection rights of employees or third parties.

Despite a company's desire to co-operate with a subpoena or production order, there may be significant legal hurdles, such as blocking statutes, preventing it from providing the material.[14] There have been several US and UK court

14 France, Switzerland, Italy and China are some of the countries that have blocking statutes. (See further, Vol. II chapters at question 60.) Breach of the Swiss blocking statute has been prosecuted on several occasions, whereas breach of the French blocking statute has, as far as is known, been prosecuted only once since its inception in 1968. However, Sapin II has a provision for penalising

decisions[15] that, applying the 'law of the forum' principle, ruled that the risk of prosecution for breaching an overseas blocking statute is not a reasonable ground for non-compliance with the court's order for discovery. In those circumstances, the company's lawyers must speak with the authority concerned, explain the issues and diplomatically suggest that the authority consider obtaining the information through the MLAT route or through police-to-police information exchange. It is vital for the company to support the process by having the material readily available, and using the contacts that the company's external lawyers might have with prosecutors in the state where the material is held, to try to expedite matters. A legitimate alternative is available if the information also exists independently in another jurisdiction, which does not have blocking statutes, provided it had been transferred there previously for valid business or legal purposes and not to get around the blocking statute.

There have been recent important legislative developments in the United States and United Kingdom that seek to make it easier for law enforcement to access electronic data held overseas. The US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) and the UK's Crime (Overseas Production Orders) Act (COPO Act) 2019 allow the authorities to compel companies, without having to apply to a court, to hand over information even where the information is held overseas. The UK–US Bilateral Data Access Agreement, signed on 3 October 2019, will lead to prosecutors gaining these additional powers. These are the first acts of the kind and reflect the theme of increased cross-border co-operation. While the impact of the legislation remains to be seen, the acts clearly represent another point at which companies can be caught between conflicting laws, with blocking statutes and data privacy laws at the other side of the pincer seeking to limit companies' ability to provide information. Companies should therefore be acutely aware of the potential for such conflicting obligations, and understand who controls their data (third parties may host or store data) and where it is stored. It is also prudent to develop plans of action for how to respond to an order to furnish evidence kept in a jurisdiction with laws prohibiting the transfer.

12.7 Concluding remarks

As explained in Chapter 11, there are many good reasons why a company might wish to take a proactive approach and voluntarily provide information rather than waiting for a subpoena or production order. It could, for example, give the best opportunity for maximising co-operation credit. Indeed, the senior UK judge granting the *Rolls-Royce* deferred prosecution agreement (DPA) cited voluntary provision of material as one of the ways Rolls-Royce demonstrated 'extraordinary'

breach of the French blocking statute, which leads some commentators to believe that it will be more readily enforced. Further, Article 48 of the GDPR has similar effect to blocking statutes across the European Union. (See further, Vol. II chapters at question 60.)

15 For example, *Secretary of State for Health and Others v Servier Laboratories and Others (Servier)* [2013] EWCA Civ 1234 and *National Grid Electricity Transmissions PLC v ABB Limited and Others* [2013] EWHC 822 (Ch).

co-operation. Depending on the facts of the case, in the authors' view, there could be little to no loss of credit by asking for a production order rather than voluntarily disclosing – if this is appropriate to overcome data protection or other barriers – provided (1) there is early dialogue with the authorities and (2) the issues are reported before the authority learns of them separately through another source.[16]

In some circumstances a company might wish to think carefully about whether it needs to demonstrate extraordinary levels of co-operation. One way to do so would be to waive legal privilege over certain classes of documents to influence the company's eligibility for the United States Department of Justice's FCPA Corporate Enforcement Policy[17] or a DPA.[18] The joint Crown Prosecution Service and SFO Guidance on Corporate Prosecutions[19] explains that 'genuinely proactive' self-reporting is a public interest factor militating against the prosecution of a company. A voluntary waiver of privilege is relevant to determining whether a company has genuinely and proactively co-operated with the SFO or other authority, and consequently to the assessment of whether it is in the public interest to prosecute or to invite the company to DPA negotiations. The SFO Corporate Co-operation Guidance states that a failure to waive privilege and provide witness accounts will not allow the company to avail itself of the corresponding factor weighing against prosecution as found in the SFO and CPS Deferred Prosecution Agreements Code of Practice[20] (but will not be penalised by the SFO). The company might therefore wish to think carefully about which documents it believes are truly legally privileged and whether in fact to assert legal privilege over them.

As stated in opening this chapter, there are many and nuanced factors to consider when a company is required to produce information to the authorities. The key is to be well prepared in terms of knowing where information is stored; to have the relevant expertise, preferably internally, to gather relevant information quickly and forensically; to have an overall strategy and end game as early in the process as possible, but also keeping things under review; and to be able to rely on trusted advisers.

16 Rolls-Royce did not self-report but still received a deferred prosecution agreement because of its 'extraordinary' co-operation. See *Serious Fraud Office v. Rolls-Royce PLC and another*, Case No. U20170036 (2017), paras. 21, 22.

17 The Corporate Enforcement Policy adapted and replaced the FCPA Pilot Program – see https://www.justice.gov/criminal-fraud/corporate-enforcement-policy. The policy includes a presumption of a declination where the company voluntarily self-reports, fully co-operates with a DOJ investigation and makes timely and appropriate remediation.

18 Of course, the implications of full or selective waiver of privilege must be very carefully thought through.

19 https://www.cps.gov.uk/legal-guidance/corporate-prosecutions.

20 https://www.cps.gov.uk/sites/default/files/documents/publications/dpa_cop.pdf.

13

Employee Rights: The UK Perspective

James Carlton, Sona Ganatra and David Murphy[1]

13.1 Contractual and statutory employee rights

13.1.1 Company policy, manual, contracts, by-laws

13.1.1.1 Suspension

The vast majority of employees implicated in an investigation will be suspended. Generally speaking, employers will rely on the increasingly common express provisions to suspend employees in the course of disciplinary investigations contained in the employment contract, staff handbook or disciplinary policies.

In the absence of such an express provision, employers may still suspend employees on the basis that it constitutes a reasonable management instruction not to work or attend the workplace in circumstances where serious allegations, particularly those of a regulatory nature, have been made or where relationships have broken down.

In such circumstances, however, employees may have greater grounds to challenge the suspension. English case law in relation to garden leave (when an employer requires an employee not to attend work during the notice period) suggests that if the employer does not have an express right to suspend an employee, the employee may have a legal basis for challenging the suspension if he or she can show that he or she needs to be able to use particular professional skills frequently to ensure that they are maintained and do not diminish through lack of use.[2] Even if the employee cannot show this, the longer the period of suspension, the more difficult it may become for the employer to justify it.

---

1 James Carlton, Sona Ganatra and David Murphy are partners at Fox Williams LLP.

2 *William Hill Organisation Limited v. Tucker* [1998] IRLR 313.

Regardless of whether it has relied on an express right or not, employers must have reasonable grounds for any suspension and these grounds should be kept under review to ensure that the period of suspension is no longer than necessary.

What constitutes a reasonable ground for suspension? 13.1.1.2

Suspension may be reasonable if the individual is suspected of serious misconduct and his or her continued attendance at work creates a potential threat to the employer's business or its other staff or could have an adverse effect on the investigator's ability to investigate the matter appropriately. In the event of a legal challenge to suspension, an employment tribunal or court is likely to consider all the relevant circumstances, including the terms of the employee's contract, what the employer has said about the suspension, the length of suspension and any financial loss it is causing.

Most employers' disciplinary procedures are not contractual, and therefore a failure to follow them does not, generally speaking, constitute a breach of contract (unless the employee can show that the failure was a breach of the implied duty of trust and confidence owed by the employer). However, in the public sector, where contractual procedures seem to be more common, there have been circumstances in which employees have successfully obtained injunctions preventing their employers from proceeding with disciplinary proceedings where to do so in the particular circumstances would constitute a breach of contract.[3]

Given the potential for disciplinary action to have significant adverse consequences on the careers and finances of employees working in regulated sectors, in the coming years we may see employees pursuing creative legal arguments to obtain injunctions against disciplinary action. Such arguments might be based on the implied duty of trust and confidence, with employees arguing that proceeding with disciplinary action in the particular circumstances would breach the duty.

In the United Kingdom, the statutory Code of Practice on Disciplinary and Grievance Procedures (the Code) published by the Advisory, Conciliation and Advisory Service (ACAS)[4] sets out the principles for handling disciplinary and grievance issues in the workplace. Its content in relation to investigations is written with internal investigations in mind, rather than investigations by an external third party, but its principles will be relevant to any disciplinary proceedings instigated by the employer and therefore to all investigations that might lead to disciplinary action. Individuals will not have any free-standing claim for any failure to follow the Code but employment tribunals take into account any such failures when considering relevant cases and the compensation to be awarded.

In practice, in a regulated environment such as the financial services sector, many employers will be far less concerned about compliance with the Code than they will be about satisfying the demands and wishes of the regulators or prosecuting authorities. Nonetheless, an individual who does not consider an investigation

3 *Mezey v. South West London & St George's Mental Health NHS Trust* [2010] IRLR 512.

4 https://www.acas.org.uk/media/1047/Acas-Code-of-Practice-on-Discipline-and-Grievance/pdf/11287_CoP1_Disciplinary_Procedures_v1__Accessible.pdf.

is being handled appropriately may find within the Code's principles some helpful points to refer to when explaining his or her concerns to the employer. In particular, that any period of suspension should be kept as brief as possible and should be kept under review.

13.1.1.3 Remuneration

It is usual for employees to continue to receive basic salary and benefits while an investigation is ongoing, irrespective of whether they are suspended from work. Unpaid suspension is rare and will not be an option open to the employer unless it has a contractual right to do so.

In the financial services sector, variable pay (such as annual bonuses and long-term incentive awards) often forms a significant part of an employee's annual remuneration and normally a proportion of variable pay is deferred and paid out over a number of years.

It is now common to see provisions in employment contracts to the effect that variable pay will not be awarded or delivered if at the time of award or delivery the individual is subject to any kind of investigation. Similar provisions are usually also found within the relevant award plan rules.

Investigations can take many years so their implementation can have a significant financial impact on the employee, particularly as it can affect deferred remuneration from prior years, as well as the current year's bonus or long-term incentive scheme award.

It is not always clear from such provisions what happens to any variable pay that is not awarded or delivered if the investigation finds there has been no wrongdoing. When negotiating employment contracts, employees should seek clarity in the wording of the provisions so they stipulate that if an investigation finds no wrongdoing, the variable pay in question be awarded or delivered.

In relation to variable remuneration awarded by banks, building societies and certain regulated investment firms, the regulatory framework contains strict restrictions for particular classes of employees.[5]

In essence, the rules are intended to discourage excessive risk-taking and encourage more effective risk management.

By way of illustration, the rules provide that, in certain circumstances, deferral (the period during which variable remuneration is withheld following the end of the accrual period) is extended to: (1) a minimum seven-year period with no vesting until three years after award for senior managers (i.e., individuals who have the greatest influence over the strategic direction of the business); (2) five years for Prudential Regulatory Authority (PRA) designated risk managers with senior, managerial or supervisory roles; and (3) three to five years for all other staff whose actions could have a material impact on a firm (material risk-takers).

5 As set out, for example, in SYSC 19D of the FCA Handbook in respect of dual regulated firms: https://www.handbook.fca.org.uk/handbook/SYSC/19D/?view=chapter.

At the same time, regulated firms must include *malus* provisions (i.e., arrangements that permit the employer to prevent vesting of all or part of deferred remuneration based on risk outcomes or performance) and clawback provisions (i.e., arrangements through which remuneration that has already vested is recouped) for seven years from the award of variable remuneration for all material risk-takers. Importantly, both the PRA and the Financial Conduct Authority (FCA) clawback rules have been strengthened by a requirement for a possible three additional years for senior managers at the end of the seven-year period where a firm or regulatory authorities have commenced enquiries into potential material failures. In effect, therefore, employees operating at a senior level in the financial services sector who are subject to an investigation potentially now face a decade of uncertainty over their pay.

Guidance from the FCA provides that, in relation to issues relating to risk-management failure or misconduct, regulated firms are expected to consider cancelling or clawing back bonus awards in relation to those employees who reasonably could have been expected to be aware of the failure, misconduct or weakness at the time but failed to take 'adequate steps' or who, by virtue of their role or seniority, were 'indirectly responsible or accountable'.[6]

A key related issue is the operation of these *malus* or clawback provisions in the context of the buy-out of awards when an employee moves from one firm to another. As a result of the regulatory framework, senior employees in the financial services sector may find that their current employer is able to apply clawback based upon the conclusions of their previous employer's investigation. As such those employees who are subject to an investigation in the regulated sector could face further uncertainty and the possibility that previous employers can determine their future pay.

English law 13.1.2

Suspended employees are bound by the express terms of their contracts and by certain terms implied by law, including a duty of fidelity (which includes a duty of confidentiality) and a duty to obey lawful and reasonable orders.

At the same time, employers are also bound by an implied duty of trust and confidence. This duty comes into play when determining whether to suspend employees implicated in misconduct.

Employees have successfully argued that a failure to consider whether suspension could be avoided was a breach of the duty of trust and confidence owed by the employer in numerous cases, paving the way for a claim for constructive dismissal.[7] Such claims are often difficult to pursue but, if successful, release the individual from any post-termination restrictions in his or her contract. Accordingly, prudent employers should keep under continuous review the need for an employee to be suspended.

6 https://www.fca.org.uk/publication/finalised-guidance/guidance-on-ex-post-risk-adjustment-variable-remuneration.pdf.

7 For example *Crawford and another v. Suffolk Mental Health Partnership NHS Trust* [2012] IRLR 402.

13.2 Representation

13.2.1 Need to collect information on behalf of client

13.2.1.1 Interviewing client

At the outset of an instruction from an individual, independent legal advisers (ILAs) should seek detailed instructions to clarify the full history of employment and determine the potential scope of the misconduct under investigation and the parties implicated. A key component of this stage is to assess the employee's relationship with the employer. Understanding the dynamics of the relationship at the outset will assist in the smooth running of the investigation and allow a better understanding of the support that is likely to be offered by the employer.

13.2.1.2 Requesting documents and information from:

Employer

An employee involved in an investigation (internal or external) may need to request that the employer provides documentation, access to witnesses or other support. This arises as during any period of suspension, the individual is often operating in a vacuum, and he or she is likely to be prohibited from having contact with clients and colleagues and prevented from having access to the employer's IT systems, documents and premises other than to the extent permitted by the employer. From an employer's perspective these restrictions are crucial to ensuring that documentation has not been compromised and that potential witnesses or accomplices have not been tipped off. Indeed, such concerns will probably be as important for the employee.

There is unlikely to be an express or implied right that the employee can rely on such support from the employer.

In the context of an internal investigation, the employer would not want to provide carte blanche access to documentation and information to the employee and is likely to prefer that the employee provide his or her own account of the circumstances.

In the context of an external investigation by law enforcement authorities, the situation is more complex. It may well be in the employer's interests to co-operate with requests for assistance to gain some understanding as to the scope of the investigation and the potential repercussions. At the same time, the employer may have its own regulatory obligations in mind and may be required to co-operate with and disclose documentation to the regulator.

Any rights of the employer to access personal electronic devices used by the employee for work are likely to be set out in the staff handbook. Generally speaking, where such devices are routinely used for work purposes, employers will be permitted to seek access to them.

Law enforcement

In circumstances where a law enforcement authority has announced its intention to interview an individual, a request for a list of questions or topics of discussion together with relevant documentation should be made to the relevant body at

the earliest opportunity. In practice, law enforcement authorities seldom provide more than a broad list of areas they wish to explore and often provide limited supporting documentation. Individuals should be advised at the outset that they are unlikely to receive detailed information from the law enforcement authority in advance of the interview and that further documentation is likely to be produced on the day of the interviews. There will be specific, limited circumstances, however, where law enforcement authorities are more receptive to such requests. For example, if the individual is no longer in employment and has no ongoing relationship with the employer or if the employer is no longer operating as a going concern, law enforcement authorities may be more amenable to requests for information as otherwise the employee will have no other avenue to properly prepare a case.

Other witnesses (and their counsel)

As noted above, individuals are likely to be prohibited from having contact with clients and colleagues during suspension. If an individual is aware of colleagues who would be able to provide assistance to clarify aspects of the case, appropriate action should be taken to contact them. Depending upon the ongoing relationship with the employer, in the first instance, it may be sensible to approach the employer to request details of the colleague's legal counsel (if one has been appointed).

Joint defence agreements 13.2.2

Between individuals and the company 13.2.2.1

On balance, in the vast majority of circumstances, co-operation between the employee and employer will be mutually beneficial. From an individual's perspective, while there is a risk of self-incrimination, co-operation with the employer allows the employee to know how the investigation is progressing and whether external regulators are involved, and grants him or her access to materials that are relevant and crucially the opportunity to engage with the employer in agreeing the outcome. Such co-operation often results in work-product produced by and communications between the parties and their legal advisers being protected by common interest privilege.

While perhaps not as frequent as in the United States, settlement discussions with law enforcement authorities in the United Kingdom are a growing trend. At the time of writing, since the introduction of deferred prosecution agreements (DPAs) in 2014, the SFO, for example, has entered into five DPAs. DPAs are not currently available for individuals in the United Kingdom. ILAs should ensure their clients appreciate the risk that the law enforcement authority may still take action against the employee in circumstances where the employer has entered into a DPA.

Between individuals and their counsel 13.2.2.2

In complex cases of misconduct, there are likely to be a number of individuals involved. There are clear advantages to ensuring communication lines are opened and maintained with ILAs engaged by potential 'co-defendants'; such

communications have the benefit of being protected by common interest privilege. The many advantages include the sharing of important information and documentation that others may have obtained, as well as the benefit of adopting a common approach with the employer to documentation requests. Employers are more likely to be receptive to common, and therefore more focused, information requests made by several employees rather than numerous different requests received at different times by each employee.

13.3 Indemnification and insurance coverage

13.3.1 Determining whether an individual is indemnified

13.3.1.1 Communications with the employer and company counsel

Upon instruction by an individual, clarification should be sought as to whether the employer will fund the costs of an ILA. From the employee's perspective, access to an ILA from the start of an investigation is essential (regardless of whether the employee is central to the allegations or on the periphery) given the potential dangers ahead. What may start off as the provision of an innocuous witness account to a regulatory authority may turn quickly into the employee being regarded as a suspect as new allegations of misfeasance surface.

13.3.1.2 Potential sources of right to indemnification

Employment contract, company policies, by-laws or local laws

It is generally very unusual to see rights of indemnification set out formally in employment contracts in the United Kingdom. In certain industries, however – for example, the financial services and media sectors – it is becoming increasingly common for employers to maintain formal policies setting out the circumstances in which they will indemnify employees' legal expenses. Such indemnification will be limited to situations where an employee is being investigated solely because of acts performed in the course of and within the scope of his or her employment.

Close attention should be paid to such policies and the restrictions set out in them. In particular, given the difficulties for an employer to determine the potential liability of an employee at the outset of an investigation, it is common for employers to provide indemnification for legal fees incurred at an initial stage while the scope of allegations is clarified and for the employer to have a right to stop further indemnification and seek reimbursement of earlier costs, for example, where the employee is found to have acted outside the scope of his or her employment.

Employers also, generally speaking, provide lists of approved law firms to act as ILAs and generally require employees to seek approval before appointing representatives not on the list.

Unlike other jurisdictions, English law does not provide indemnification rights to employees.

Insurance policies of employer

D&O insurance

At the same time, employees at a senior level may also benefit from directors' and officers' (D&O) insurance.

The coverage of D&O policies should be carefully considered from both the employee's and employer's perspective to ensure that the policy covers investigations, prosecutions and related civil claims.

Generally speaking, UK-based D&O policies provide cover for 'formal' investigations. ILAs should clarify whether the definition of investigations also includes internal investigations and consider why the investigation has commenced. If an internal investigation has been commenced by the employer, for example, as a result of concerns over its own conduct and liability, other insurance policies, such as professional indemnity insurance, might be engaged. At the same time, the D&O policy might include an exclusion in relation to claims in connection with the performance or failure to perform professional services by or on behalf of any director or officer. In such circumstances, the professional indemnity insurance policy should become engaged. The exclusion of the D&O insurance and application of professional indemnity (or other related) insurance is frequently debated at the outset of investigations, particularly where there is concern about the requirement to pay deductibles under the D&O policy or where there are local insurance requirements under a global policy.

Advocating for indemnification when not otherwise clear 13.3.2

From the employer's perspective, the appointment and funding of an ILA has clear benefits where it appears that the interests of both parties are congruent. It encourages the co-operation of the employee and assists in ensuring that certain communications with the employee can be made with the protection of privilege. See Section 13.4

While indemnification policies are becoming more common, many employers choose not to have a formal policy and instead seek to enter into separate arrangements at the time of the investigation. This approach is attractive from the employer's perspective as it enables the employer to select when and how it will indemnify certain individuals without setting a precedent. In such circumstances, the employee should negotiate carefully to ensure that all potential costs and eventualities are covered.

Awareness of situations where indemnification may cease 13.3.3

Violation of undertaking to the company 13.3.3.1

Employer policies will set out the circumstances in which indemnification will cease. A common provision is the employee acting contrary to restrictions and requests set out in the agreement. For example, the indemnification policy or agreement may contain clauses requiring the employee to act in good faith in its dealings with the employer and regulatory authorities or to provide updates to the employer at given stages. Such undertakings should be highlighted in advance to

individuals and ILAs should ensure that information is provided to the employer and its counsel.

It is important to advise individuals at the outset that violation of certain provisions may also lead to the employer seeking reimbursement or clawback of fees already incurred.

13.3.3.2 Failure to co-operate with investigation

How to decide whether to co-operate where failure to do so will affect indemnification

Most indemnification policies or agreements will contain provisions setting out the need for full co-operation between the employee and employer. At various stages of an investigation, the employee should consider carefully whether it continues to be in his or her best interests to fully co-operate with the employer. As the investigation develops, matters may come to light that indicate the employee's interests conflict, or are likely to conflict, with the employer's. In such circumstances, ILAs should discuss with the employee whether co-operation remains in the employee's best interests and the consequences that will flow from adopting a stance that is at odds with the employer.

13.3.4 Ensuring sufficient funds for protracted investigation

13.3.4.1 Cap on insurance policy

D&O policies should be reviewed at the outset and during investigations to ensure the scope and limitations of coverage are understood.

Generally, D&O policies include annual or total aggregate limits, or both. In circumstances where the employer and a number of directors are under investigation or where investigations are becoming protracted, it is not uncommon for the aggregate limit to quickly become exhausted. ILAs should ensure that the scope of any insurance cover is kept under constant review.

13.3.4.2 Commitment of company to continue indemnification

As previously noted, employers will continually assess whether it is appropriate to continue to indemnify employees under investigation. If it becomes clear that the employee has acted outside the scope of employment, the employer is unlikely to continue to provide support unless it would be in its interests to do so because, for example, there is a potential for related civil claims to be made against the employer.

13.4 Privilege concerns for employees and other individuals

13.4.1 In communications with other employees

13.4.1.1 Colleagues or people involved in underlying events

See Chapter 35 on privilege

As a matter of English law, communications between an ILA and third parties will only be protected by privilege if they relate to an existing, pending or reasonably contemplated litigation (in other words, litigation privilege applies). This

is not always going to be the case in the context of an internal, or indeed external, investigation.

As such, unless the former colleague or associate of the individual is also implicated in the allegations such that common interest privilege may arise in discussions involving their ILA, ILAs should avoid communicating with third parties. Even in circumstances where common interest privilege can be said to arise, this is a developing area of English law and therefore subject to change. ILAs should act with caution and ensure that the common interest between the parties is clearly recorded at the outset.

Company counsel 13.4.1.2

Communications between the employee and legal counsel instructed by the employer will not be privileged unless common interest privilege exists. Whether it exists will depend on the circumstances; even if it does, it will not necessarily encompass all communications with counsel.

Interviews conducted during internal investigations by the employer will not be privileged from the employee's perspective; the privilege, if it exists, lies with the employer.[8]

See Chapter 35 on privilege

Use of employer email to conduct privileged conversations 13.4.2

With internal counsel 13.4.2.1

Employees should be wary of any communications with in-house counsel as such communications are unlikely to be protected by privilege.

See Chapter 35 on privilege

Unless the individual forms part of the client group identified within the employer[9] or unless litigation privilege applies, communications with the in-house counsel will not be protected by privilege.

With external counsel 13.4.2.2

Communications between an individual and an ILA will of course be protected by legal advice privilege. However, there are circumstances in which that privilege may be lost, particularly if it can be shown that the confidentiality in the communication has been lost as it is accessible by third parties.

On balance, it is inadvisable for an employee to use work email accounts to communicate with an ILA as it is likely (depending on the terms of any relevant IT policy maintained by the employer) to lead to a dispute that confidentiality in those communications has been lost.[10]

8 The case of *R (on the Application of AL) v. SFO* [2018] EWHC 856 (Admin) highlights the fact that the SFO is likely to be under increasing pressure to seek waiver of privilege over interview notes for disclosure in subsequent criminal prosecutions.

9 As required following *Three Rivers District Council v. Bank of England* [2003] EWCA Civ 474.

10 In *Shepherd v. Fox Williams LLP* and others [2014] EWHC 1224 (QB) it was held that the claimant remained entitled to assert privilege over documents even though they had been accessible to the defendant employer when they were sent to the work email address of an employee of the defendant.

14

Employee Rights: The US Perspective

Milton L Williams, Avni P Patel and Jacob Gardener[1]

14.1 Introduction

Unless required to by contract or subpoena, employees and former employees may decline to provide information or documents in connection with a corporate investigation. However, many employers will insist on employee co-operation and may impose disciplinary measures – up to and including termination – on those employees who refuse.[2] In the absence of contractual protections, employees may have no legal right to refuse to submit to an interview, even if their answers tend to incriminate them. A 2016 decision from the United States Court of Appeals for the Second Circuit in *Gilman v. Marsh & McLennan Companies, Inc*[3] is instructive. There, two employees argued that Marsh & McLennan's demand they submit to an interview in an internal investigation constituted state action that infringed their right against self-incrimination. The court rejected this argument, calling it 'the legal equivalent of the "Hail Mary pass" in football'.[4]

---

1 Milton L Williams is a partner, Avni P Patel is a senior associate and Jacob Gardener is an associate at Walden Macht & Haran LLP.

2 See Testimony of Henry W Asbill, National Association of Criminal Defense Lawyers, to the US Sentencing Commission, at 4 (15 November 2005) ('Increasingly, companies do not hesitate to fire individual employees who refuse to "cooperate".'); Sarah Helene Duggin, Internal Corporate Investigations: Legal Ethics, Professionalism, and the Employee Interview, 2003 Colum. Bus. L. Rev. 859, 907 (2003) ('[I]n most states, [an employee's] refusal to cooperate with an internal investigation "constitutes a breach of the employee's duty of loyalty to the corporation and is good grounds" [for dismissal.]').

3 826 F.3d 69 (2d Cir. 2016).

4 826 F.3d at 76 (internal quotation marks omitted). In exceptional circumstances, where the government exerts overwhelming influence over the internal investigation and the employer's decision-making, the employer's actions may be found to constitute state action. See, e.g., *United States v. Stein*, 541 F.3d 130, 136 (2d Cir. 2008) (holding that 'KPMG's adoption and

Although employees generally cannot refuse to participate in investigations without risking their employment, they do possess various rights implicated by corporate investigations. The sources of those rights include the employer and federal and state law. With respect to the employer, many companies have policies and procedures for internal investigations. For instance, employee handbooks, company by-laws, written guidelines and employment agreements often contain provisions regarding employee data and document collection, workplace searches, communication monitoring, privacy and confidentiality. These documents may also provide guidance on an employee's right to indemnification for legal fees expended during an investigation or related proceedings. In addition, many companies maintain written policies that protect employees from retaliation for participating in an investigation. These documents, and unwritten, established company procedures, should be considered to understand the protection afforded to employees in an investigation.

Federal and state law also govern the rights of employees involved in investigations. These rights, discussed below, can be divided into three general categories: (1) the right to be free from retaliation; (2) the right to representation; and (3) the right to privacy.

The right to be free from retaliation 14.2

Although employees generally have no right to refuse to participate in a corporate investigation, they may be protected from retaliation. A number of federal employment statutes prohibit retaliation against employees who participate in corporate investigations.[5] State and local laws provide similar protection.

Moreover, employees who possess information regarding corporate misconduct have some leverage in that they may become whistleblowers. Whistleblowers are protected from retaliation under federal[6] and state whistleblower laws.

See Chapter 20 on whistleblowers

The Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley) provides for both civil and criminal penalties for employers who retaliate against whistleblowers. Section 806 of the law governs civil penalties. It prohibits publicly traded companies from retaliating against employees who assist or provide information to law enforcement, Congress, or 'a person with supervisory authority over the employee' regarding activity the employee reasonably believes is a violation of: (1) federal law regarding mail, wire, securities, or bank fraud; (2) an SEC rule or regulation; or (3) any provision of federal law relating to fraud against shareholders.[7]

---

enforcement of a policy under which it conditioned, capped and ultimately ceased advancing legal fees to defendants followed as a direct consequence of the government's overwhelming influence, and that KPMG's conduct therefore amounted to state action').

5 These statutes include Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Fair Labor Standards Act, the Family and Medical Leave Act, the National Labor Relations Act, and the Occupational Safety and Health Act.

6 The Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley), the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), the Consumer Financial Protection Act of 2010.

7 See 18 U.S.C. § 1514A(a).

Section 1107 of Sarbanes-Oxley provides for criminal penalties for retaliation against whistleblowers. Specifically, it criminalises '[w]hoever knowingly, with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense'.[8]

Section 922 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) provides anti-retaliation protection for whistleblowers who report possible securities law violations to the Securities and Exchange Commission (SEC).[9] Similarly, Section 748 of Dodd-Frank protects whistleblowers who report violations of the Commodity Exchange Act to the Commodities Futures Trading Commission.[10] And Section 1057, which codifies the Consumer Financial Protection Act of 2010, forbids retaliation against employees who blow the whistle on possible violations of that statute.[11]

Despite their similarities, there are important differences between the whistleblower protections contained in Sarbanes-Oxley and Dodd-Frank. Procedurally, in contrast to Sarbanes-Oxley's requirement that complaints be filed with the Department of Labor within 90 days of the retaliatory action, Dodd-Frank permits an employee to bring a private cause of action directly, without having to go through an administrative agency,[12] and allows the employee to do so within six to ten years, depending on the circumstances.[13] In addition, Dodd-Frank provides more attractive financial incentives for whistleblowers. A whistleblowing employee who prevails under Dodd-Frank may receive up to twice the amount of wages lost due to retaliation, as well as attorneys' fees.[14]

Under Sarbanes-Oxley, by contrast, a whistleblower's recovery is limited to the 'relief necessary to make the employee whole', including reinstatement, back pay, 'special damages' (which includes damages for non-economic harm such as reputational injury, mental anguish and suffering), attorneys' fees and costs.[15]

Critically, however, whereas Sarbanes-Oxley protects employees who report concerns to supervisors at their company, Dodd-Frank does not. Dodd-Frank defines 'whistleblower' to mean a person who provides 'information relating to a violation of the securities laws to the Commission'.[16]

---

8 See 18 U.S.C. § 1513(e).

9 See 15 U.S.C. § 77a.

10 See 7 U.S.C. § 26.

11 See 12 U.S.C. § 5567.

12 See 15 U.S.C. § 78u-6(h)(1)(B)(i).

13 See 15 U.S.C. § 78u-6(h)(1)(B)(iii)(I)-(II).

14 See 15 U.S.C. § 78u-6(h)(1)(C).

15 See 18 U.S.C. § 1514A(c).

16 See 15 U.S.C. § 78u–6(a)(6). The Supreme Court has held that this provision requires whistleblowers to report to the SEC. See *Digital Realty Tr., Inc. v. Somers*, 138 S. Ct. 767, 776, 778 (2018). Dodd-Frank's requirement that whistleblowers report information to the SEC for the anti-retaliation provisions to apply may soon be eliminated. On 9 July 2019, the US House of Representatives passed HR 2515, also known as the Whistleblower Protection Reform Act of 2019.

The right to representation 14.3

Employees have no automatic right to counsel during an internal investigation,[17] unless contractually provided under the terms of their employment.[18] Nonetheless, employees may choose to retain counsel, particularly if they face liability.

Concerns over individual criminal liability have increased since September 2015, when then-Deputy Attorney General Sally Yates issued a memorandum titled 'Individual Accountability for Corporate Wrongdoing'. The 'Yates Memo' stresses the importance of combating corporate misconduct by holding individuals accountable. It lists six steps that should be part of all investigations and prosecutions of corporate misconduct, the first of which is that a corporation's eligibility for co-operation credit depends on it providing the Department of Justice (DOJ) with all relevant facts about the individuals involved in the alleged misconduct. The Yates Memo also states that all investigations must focus on individuals from the inception of the investigation, and that barring extraordinary circumstances, which must be personally approved in writing by specified DOJ personnel, DOJ attorneys will not agree to any settlement or corporate resolution that dismisses charges or provides immunity for individual officers or employees.[19]

The bipartisan bill would amend Dodd-Frank to clarify that whistleblowers who report misconduct to their employers and not to the SEC also have protections against retaliation under the law.

17 The Sixth Amendment right to counsel is triggered by a custodial interrogation by law enforcement authorities. See *Miranda v. Arizona*, 384 U.S. 436, 479 (1966). An internal investigation by a private company does not generally implicate this right.

18 Union employees, however, may insist that a union representative attend any investigatory interview that could lead to the employee's discipline. See *N.L.R.B. v. J. Weingarten, Inc.*, 420 U.S. 251, 256 (1975). The union representative may not interfere with the interview. *New Jersey Bell Tel. Co. & Local 827, Int'l Bhd. of Elec. Workers, Afl-Cio*, 308 NLRB 277, 279, 280 (1992). Employers have no obligation to inform employees of their right to union representation or to ask if they would like a union representative present during the interview.

19 The US Department of Justice under President Trump has reaffirmed the importance of prosecuting individual wrongdoers in corporate investigations. However, in a speech given in November 2018, Deputy Attorney General Rod J Rosenstein announced an updated policy to 'make clear that investigations should not be delayed merely to collect information about individuals whose involvement was not substantial, and who are not likely to be prosecuted.' Department of Justice News, 'Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act' (29 November 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0. In addition, on 20 November 2019, the DOJ announced changes to its Foreign Corrupt Practices Act Corporate Enforcement Policy, which now requires, among other things, companies seeking co-operation credit to disclose 'all relevant facts known to [them] at the time of disclosure . . . as to any individuals substantially involved in or responsible for the misconduct at issue' (the previous version required companies to disclose 'all relevant facts' regarding individuals substantially involved in a 'violation of law') and to alert the DOJ of evidence of the misconduct when they become aware of it (previously, companies had to disclose evidence they were or should have been aware of). See Justice Manual, 9-47.000, https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977.

14.3.1 Interviews without employee's counsel

An employer may seek to conduct an interview of an employee, either with or without company counsel present, before that employee has appointed counsel.[20] Once the employee offers an account of events, it may be difficult to offer a different one later. When counsel for individuals are appointed, they should obtain all information regarding their clients' prior statements about the subject of the investigation, including requesting any relevant memoranda created in prior interviews. Individual counsel should also request all documents, data and other information pertaining to their clients' involvement in the subject of the investigation. Requests for such information may be directed to the client, company counsel, law enforcement and other witnesses (or their counsel). Even if counsel is not allowed to participate in a client's investigatory interview, they should use the acquired information to prepare their clients.[21]

During an interview with no employee counsel, the employee may ask whether he or she should obtain individual counsel. This can place the interviewer in an uncomfortable position. An affirmative answer could have undesirable consequences, including delaying the investigation, chilling the employee's candour, and risking that individual counsel may approach law enforcement before the employer concludes the internal investigation. A negative answer creates complications and potential claims against the employer and investigating counsel if the employee self-incriminates or compromises future legal positions during the interview. Generally, the prudent course is to politely decline to answer the question.

Employers often wish to disclose to the government information obtained from employees during investigatory interviews to obtain co-operation credit or general goodwill. However, in the absence of instructions to the contrary, interviewed employees may believe that their company's attorneys represent them, and may attempt to assert attorney–client privilege over their communications with company counsel. To avoid this problem, counsel should provide an *Upjohn* warning at the start of any interview, and delivery of the warning should be documented by a note-taker.

See Chapter 8 on witness interviews and Chapter 16 on representing individuals in interviews

14.3.2 Separate representation arranged by the employer

Whether the employer agrees to arrange for counsel can depend on a number of factors, such as the employee's contractual and indemnification rights, the

20 If individual counsel is retained, company counsel must be cognisant of Model Rule of Professional Conduct 4.2, which states: 'In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order.'

21 If counsel concludes, after reviewing the available information and conferring with the client, that the evidence establishes the client's guilt, counsel may wish to advise the client to decline an interview to avoid making potentially incriminating statements. Although that may prompt the client's termination, counsel may reasonably determine that termination is inevitable regardless of the client's participation in the interview.

corporate by-laws, and the potential conflict of interest between the employee and the corporation. Although separate representation of an employee can increase expenses and lengthen the investigation, it can also provide certain advantages to the company. It can reduce any suggestion of improper influence by the company over the employee, which can bolster the company's credibility with the government when reporting the results of the investigation and increase the company's co-operation credit. In some circumstances (particularly when individual counsel has a good working relationship with company counsel), it can facilitate communication with the employee. Company and individual counsel should come from different law firms. Further, arranging for individual representation can deter the government from communicating directly with the employee.

When confronted with multiple employees who warrant separate counsel, employers may seek to reduce costs by arranging for 'pool counsel' to represent the entire group. However, this pool arrangement must be reassessed if a conflict of interest arises within the group.

The right to privacy 14.4

Workplace searches 14.4.1

In most circumstances, an employer can conduct searches of its workplace and computer system to investigate wrongdoing. Such searches are largely unprotected by personal privacy laws as workspaces, computer systems and company-issued electronic devices are generally considered to be company property. Many companies explicitly address this in written corporate policies and employment agreements. However, unwarranted or unreasonable invasions of privacy during a workplace search may be protected under state law – including state constitutional,[22] statutory[23] and common law.[24]

Employees who use their own personal electronic devices for work should be aware that work-related data stored on those devices belongs to the employer. Therefore, employees are advised to refrain from using their personal devices for work, and instead maintain separate work devices. If an employer seeks to obtain or review work-related data from an employee's personal device, the employer must be careful to exclude any personal data.

22 See, e.g., Cal. Const. art. I, § 1 (protecting right to privacy).

23 See, e.g., Cal. Lab. Code § 980 (2012) (prohibiting an employer from requiring or requesting an employee to: (1) '[d]isclose a username or password for the purpose of accessing personal social media', (2) '[a]ccess personal social media in the presence of the employer', or (3) '[d]ivulge any personal social media, except' in response to a request 'to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding'; prohibiting an employer from taking adverse action against an employee or applicant for not complying with a prohibited request or demand for access to social media).

24 See, e.g., claims for invasion of privacy, intentional infliction of emotional distress and negligent infliction of emotional distress.

14.4.2 Workplace surveillance

An employer seeking to investigate wrongdoing through electronic surveillance must be mindful of federal and state law.

Title III of the federal Omnibus Crime Control and Safe Streets Act of 1968[25] criminalises the intentional interception of any wire, oral or electronic communication unless at least one of the parties to the communication has consented to such interception or the employer is monitoring or recording employee telephone calls 'in the ordinary course of its business'.[26]

Most states (and the District of Columbia) similarly prohibit electronic surveillance of communications unless at least one party to the communication provides consent. Some, but not all, of these jurisdictions provide exemptions for employer monitoring of employee communications. Eleven states – California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania and Washington – prohibit (either criminally or civilly) surveillance without the consent of all the parties to the communication.[27]

Notably, with respect to email, because employees generally do not possess an expectation of privacy in their work accounts, employers may access personal emails exchanged over these accounts. Employees should be aware that some employers may choose to install surveillance monitoring systems into work accounts, databases and company-provided devices. As technology and communications systems advance, employees should also be conscious of their activities on communications platforms. Some messenger services used by companies, such as Slack, have recently announced new privacy policies that allow employers to download all data from their workspace, including all employee data and messages.

14.4.3 Polygraph testing

An employer's use of polygraph testing in aid of an investigation is limited by the Employee Polygraph Protection Act of 1988.[28] An employer seeking to use a polygraph must: (1) be conducting 'an ongoing investigation involving economic loss or injury to the employer's business, such as theft, embezzlement, misappropriation, or an act of unlawful industrial espionage or sabotage'; (2) possess 'a reasonable suspicion that the employee was involved in the incident or activity under investigation'; (3) show that 'the employee had access to the property that is the subject of the investigation'; and (4) follow a number of statutorily mandated procedural guidelines.[29] If the employer satisfies these requirements, it can terminate

25 See 18 U.S.C. § 2510 et seq.

26 See 18 U.S.C. § 2510(5)(a).

27 See Cal. Penal Code § 632 (a)-(d); Conn. Gen. Stat. Ann. § 52-570d; Fla. Stat. Ann. §§ 934.01 to .03; 720 Ill. Comp. Stat. ANN. § 5/14-1, -2; Md. Code Ann. Cts. & Jud. Proc. § 10-402; Mass. Gen. Laws Ch. 272, § 99; Mont. Code Ann. § 45-8-213; Nev. Rev. Stat. § 200.620; N.H. Rev Stat. Ann. §§ 570-A:2; 18 Pa. Cons. Stat. §§ 5702, 5704; Wash. Rev. Code §§ 9.73.030 to 9.73.230.

28 See 29 U.S.C. §§ 2001-2009.

29 See 29 U.S.C. § 2006(d).

an employee who refuses to take the polygraph test, or takes it and fails, provided there is 'additional supporting evidence' justifying the termination.[30]

The Secretary of Labor may bring court action to restrain employers who violate the statute and may assess monetary penalties. In addition, an employer who violates the law may be liable to the employee or prospective employee for appropriate legal and equitable relief, which may include employment, reinstatement, promotion, and payment of lost wages and benefits.

State law may provide additional restrictions on the use of polygraph tests and other tests purporting to determine truth or falsity.[31]

Indemnification 14.5

Among the significant issues that may arise from in-house counsel, and often external counsel, representing the company and not the individual is whether the employee has a right to be indemnified. The right to be indemnified may extend to legal fees, advancement of legal fees and for any potential judgment debt or settlement. As discussed above, an employee has a right to have his or her own counsel, even if the company pushes for joint representation by company counsel, but the complicated question of whether the company must indemnify the employee for costs around separate representation may arise. Determining a company's indemnification obligations requires close review of any agreements and understandings that might give rise to indemnification or advancement of fees. It is critical that an employee communicate closely with company counsel to come to a mutual understanding of the company's obligations.

Determining whether an individual is indemnified 14.5.1

Employees should ask their counsel to assertively engage in communications with the employer and company counsel to determine whether the company will agree to indemnify the individual employee and to advance fees. This conversation should also specifically discuss the exact scope of any indemnification. If the company agrees to, or must, indemnify from any agreement or source of this right, employee's counsel should draft and execute a written agreement binding the company. Although the company may seek to impose unfavourable terms, it is generally advisable to reduce the indemnification obligation to writing.

Employees and their counsel should carefully review potential sources of the right to indemnification. These sources may include company by-laws, local law in the state of incorporation, company policies and insurance policies of the employer.

30 See 29 U.S.C. § 2007.

31 See, e.g., N.Y. Lab. Law §§ 733, 735 (prohibiting employer from using 'psychological stress evaluator examination' to determine truth or falsity); Cal. Lab. Code § 432.2 (prohibiting employers from 'demand[ing] or requir[ing] any applicant for employment or prospective employment or any employee to submit to or take a polygraph, lie detector or similar test or examination as a condition of employment or continued employment').

14.5.2 Potential sources of right to indemnification

14.5.2.1 Corporate by-laws

Corporate by-laws often delineate the company's obligation to indemnify an employee's costs arising out of representation for internal investigations or any matters related to his or her official duties. Employee counsel must carefully review corporate by-laws because, even if indemnification obligations are provided, they are often listed with limitations or releases from obligation. For example, many companies include release provisions releasing the company from its obligations or entitling it to repayment of any indemnified cost if the costs subsequently transpire not to be indemnifiable. If these provisions exist, it is likely that the company will require the employee to sign an undertaking letter, in which the employee agrees to repay any amounts advanced if it is later determined that the employee was not entitled to indemnification. Similarly, there is a difference between the duty of an employer to indemnify an employee of costs incurred and any duty to advance defence costs. Some corporate by-laws regarding indemnification may require advancement of attorneys' fees. However, the by-laws should be reviewed carefully, because absent such language, the employee has no right to advancement of attorneys' fees.[32]

Many corporate by-laws also include specific language of which employee categories have a right to indemnification. For example, it is common for company by-laws to indicate that the company must indemnify an officer or director who is successful on the merits or otherwise in the defence of a qualifying claim, but remain silent on the issue of whether other private employees have a right to indemnification. These other employees, or their attorney, should ask for indemnification whenever a claim or investigation arises.

14.5.2.2 Local law in state of incorporation

Employees and their counsel should also review state and local laws in the state of incorporation. Review of state and local laws is often overlooked because employees assume indemnification provisions are exclusively contained in corporate by-laws and any employment or subsequent agreements with the company. However, a number of states impose indemnification obligations on companies in local and state laws for private employees, especially for directors and officers.

Under Delaware corporate law, directors generally have a right to indemnification if they are, or face being, parties to a proceeding or subject to investigation, unless they did not act in good faith and in a manner reasonably believed to be in, or not opposed to, the best interests of the corporation.[33] Directors and officers who succeed in their defence are indemnified. On the other end of the permissive spectrum, if a director or officer acts in 'bad faith', they are not entitled to indemnification. Delaware courts have stated that the 'boundaries for indemnification'

32 In practice, more often than not, by-laws will entitle employees to have their attorneys' fees advanced.

33 See 8 Del. C. § 145(c).

are 'success' and 'bad faith'.[34] To determine where on the permissive spectrum their situation lies, directors and officers should turn to any governing documents for additional language. Delaware law also allows directors and officers the right to indemnification through advanced costs for pending litigation.[35]

Both Oregon and Washington law also provide for mandatory indemnification of a director who successfully defends, on the merits or otherwise, any proceeding in which the director was made a party due to his or her position as a director with the company, unless the articles of incorporation provide otherwise.[36]

California is an example of a state that extends indemnification protections to any private employee, not only directors or officers. The California Labor Code provides that an employee has a right to reimbursement. The obligation is found in California Labor Code Section 2082, which states:

> *Any employer shall indemnify his or her employee for all necessary expenditures or losses incurred by the employee in direct consequence of the discharge of his or her duties, or of his or her obedience to the directions of the employer, even though unlawful, unless the employee, at the time of obeying the directions, believed them to be unlawful.*[37]

The California Supreme Court explained the statute's application to indemnification as a public policy obligation. In *Edwards v. Arthur Andersen LLP*,[38] the Court stated:

> *California has a strong public policy that favors the indemnification (and defence) of employees by their employers for claims and liabilities resulting from the employees' acts within the course and scope of their employment. Labor Code section 2082 codifies this policy and entitles employees to indemnification from their employer.*

Company policies 14.5.2.3

Employees should also look at company policies and employment contracts or subsequent agreements as sources of indemnification rights. In addition to indemnification required by corporate law, individual employees may have contractual indemnification rights in their employment agreements. Even if the company by-laws do not indicate a right to indemnification, a company must honour any obligations in individual employment agreements. For example, as good business practice and to promote co-operation with an investigation, some companies may decide to expand the scope of indemnity to include employees who might not be covered by the by-laws or state and local laws that are likely to be witnesses

34 *Hermelin v. K-V Pharm. Co.,* 54 A.3d 1093, 1094 (Del. Ch. 2012).

35 See 8 Del. C. § 145(e).

36 See ORS 60.394 and RCW 23B.08.520.

37 See Cal. Labor Code § 2802(a).

38 44 Cal. 4th 937, 952 (2008).

or subjects. As a strategic point, employers may expand the scope of indemnity to ensure co-operation of employees, which may show the company in a more favourable light to any regulator or investigative body.

14.5.2.4 Insurance policies of employer

Some employers may choose to purchase directors' and officers' (D&O) insurance to supplement or provide an alternative to indemnification. Some indemnification agreements require companies to purchase insurance. If the employer has D&O insurance, the nature of the allegation and the terms of the specific policy may trigger payment of defence costs.

D&O insurance is increasingly important in corporate culture owing to the increase in shareholder, class action, derivative action and other prosecutorial and regulatory investigations targeting not only companies, but also their directors and officers. If any employee is also a director or officer of the company, it is important to understand that D&O insurance policies are not standard and can vary in terms of protection. It is crucial for employees and their counsel to review terms, conditions, provisions and exclusions.[39]

14.5.3 Advocating for indemnification

Despite numerous possible sources giving rise to the right to indemnification, companies are not always eager to indemnify employees for representation or costs incurred during an investigation or defence. However, employees should advocate for the company to indemnify them for incurred costs or advancement of fees. The benefits to both the employer and employee should be emphasised, as indemnification can protect both parties' interests. When entering an employment or separation agreement, an employee should request and push for a specifically defined indemnification provision.

The employer or company may become more credible and promote efficiency and effectiveness of an internal investigation by ensuring that employees are adequately represented. If company counsel recognises a conflict of interest and the need for the employee to have separate representation, the corporation benefits if the employee is co-operative. Therefore, the company may assess the employee's involvement and whether failure to pay individual counsel fees or to advance attorneys' fees will make the employee's co-operation less likely. While in some instances employees may be required to co-operate by subpoena, it is in the best interest of the corporation to work jointly with the employee to prepare its own defence and receive information in advance through a joint defence agreement.

In addition, regulators and prosecutors cannot take into account during an investigation whether a corporation is advancing or reimbursing attorneys' fees or providing counsel. Along the same lines, a prosecutor or regulatory body cannot request that a company refrain from taking such action. In 2008, the

39 See generally Matthew L Jacobs, Julie S Greenber, *Basic Principles of D&O Coverage and Recent Developments*, 741 PLI/Lit 29, *35 (2006).

Department of Justice published the 'Filip Memo',[40] which laid out the principles of federal prosecution of business organisations. The guidelines, codified in the US Attorney's Manual (now called the Justice Manual), state that: 'In evaluating cooperation, however, prosecutors should not take into account whether a corporation is advancing or reimbursing attorneys' fees or providing counsel to employees, officers, or directors under investigation or indictment.'[41]

Situations where indemnification may cease 14.6

Employees should be aware of the circumstances in which a company's obligations to indemnify may cease. As mentioned above in Section 14.5, a company's obligations to indemnify an employee may be contingent on, and circumvented by, any undertaking agreement between the parties. An undertaking agreement requires an employee to repay any advanced or covered costs in the event the costs were ultimately not deemed indemnifiable. A company is generally released from its indemnification obligations for any violation of an undertaking agreement (substantive or procedural) and fraud or bad faith.

Failure to co-operate with investigation

See Chapter 10 on co-operating with authorities

In some instances, an employee's failure to co-operate with a company's investigation could absolve the company's obligation to cover individual costs. This can create a difficult decision for an individual employee regarding whether to co-operate where failure to do so will affect indemnification. Even if an employee does not want to co-operate with company counsel – internal or external – and submit to an interview or otherwise co-operate, he or she may still be called to produce testimony or information pursuant to a subpoena. Failure to initially co-operate may preclude an employee from securing indemnification for assumed costs. However, it is still often in the best interest of an employer to offer to indemnify employees who may initially seem unco-operative, because in the event they are called to testify, it is probably safer for the company if they are represented.

Privilege concerns for employees 14.7

Privilege considerations become central during investigations. Because of the various permutations of attorney–client relationships with both internal and external counsel, it is important for employees to remember that they only enjoy protections over communications with individual counsel. If an employer requests an interview with an employee, employee counsel and company counsel, the communications and testimony at the interview are not privileged.

40 Memorandum from Deputy Attorney General Mark Filip to Heads of Department Components and United States Attorneys, Principles of Federal Prosecution of Business Organizations 8 August 2008), available at https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf.

41 USAM 9-28-730 Obstructing the Investigation.

An employee and his or her counsel should note whether the company counsel issued a proper *Upjohn* warning and whether it was documented. If an inadequate *Upjohn* warning was given, an employee's individual counsel may attempt to prevent or limit disclosure of any statements made by the employee in an interview where individual counsel was not present.

The Third Circuit established the *Bevill* standard to determine whether a company employee holds a joint privilege with the employer company over communications with corporate counsel, which has since been adopted by the First, Second, Ninth and Tenth Circuits. The *Bevill* standard holds that 'any privilege that exists as to a corporate officer's role and functions within a corporation belongs to the corporation, not the officer'.[42] The Court in *Bevill* extended the privilege to officers and employees in an individual, personal capacity only when the employee satisfies the following five-factor test. First, they must show that they approached counsel for the purpose of seeking legal advice. Second, they must show that when they approached counsel, they made it clear that they were seeking legal advice in their individual capacity rather than in their representative capacities. Third, they must demonstrate that the counsel saw fit to communicate with them in their individual capacities, knowing that a possible conflict could arise. Fourth, they must prove that their conversations with counsel were confidential. And fifth, they must show that the substance of their conversations with counsel did not concern matters within the company or the general affairs of the company.[43] Notwithstanding the foregoing, an employee would be ill-advised to confide in, or speak candidly with, company counsel given the subjective nature of the standard. Whenever possible, an employee should make efforts to secure personal individual counsel.

See Chapter 8 on witness interviews and Chapter 16 on representing individuals in interviews

Finally, as a practical matter, employees should be aware that communications with other employees or colleagues regarding the investigation are not privileged regardless of whether the colleague is also involved in the investigation or represented by the same counsel. Even if an employee believes he or she is sharing attorney communications with other employees who need to know the attorney's advice and who also have an attorney–client privilege with the same counsel because he or she is involved or implicated in the investigation and also represented by company counsel, it is always prudent to refrain from sharing privileged information. If an attorney's communication is shared beyond those who need to know, the attorney–client privilege, may be destroyed. In addition, employees should attempt to communicate with individual counsel on personal and non-company devices to ensure that the privilege is protected.

See Chapter 35 on privilege

42 *In re Bevill, Bresler & Schulman Asset Mgmt. Corp.* 805 F.2d 120 (3d Cir. 1986).

43 *US v. Graf*, at 8 (citing *Bevill,* 805 F.2d 120 (3d Cir. 1986)).

15

Representing Individuals in Interviews: The UK Perspective

Jessica Parker and Andrew Smith[1]

Introduction 15.1

This chapter considers the representation of individuals in three types of interviews: interviews in corporate internal investigations, interviews of witnesses in law enforcement investigations, and interviews of suspects in law enforcement investigations.[2]

Interviews in corporate internal investigations 15.2

When should employees have their own lawyer? 15.2.1

In many corporate internal investigations, it is common for employees not to receive or be offered legal advice, either before or during their interviews. This is because the employee is not normally treated as a suspect in what is commonly referred to as a 'fact-finding investigation'. Their position is analogous to but distinct from an employee interviewed in disciplinary proceedings, in which an employee suspected of misconduct has no right to legal representation at the interview, but is usually entitled to be accompanied by a fellow employee or trade union representative.

However, in some corporate internal investigations, the corporate may recommend a lawyer (often called an independent legal adviser or ILA) who can represent

1 Jessica Parker and Andrew Smith are partners at Corker Binning.

2 By 'law enforcement investigations' we mean investigations by UK public bodies such as the National Crime Agency and regional police forces exercising a statutory function of investigating criminal offences. Some of these bodies also act as prosecutors, for example the Serious Fraud Office and the Financial Conduct Authority. In other cases, the Crown Prosecution Service will be responsible for prosecuting. There are other types of interviews in law enforcement investigations which fall outside the scope of this chapter, for example interviews of co-operating witnesses under the Serious Organised Crime and Police Act 2005.

the employee. Alternatively, the employee may prefer to benefit from legal advice, regardless of whether a lawyer has been recommended by the corporate.

Legal representation for an employee may be desirable in two main situations. First, if the employee risks self-incrimination or admitting regulatory breaches, there may be a conflict of interest between the employee and the corporate. In particular, conducting the interview without first offering the employee legal representation may place the corporate's lawyers in breach of their professional ethical duty not to take 'unfair advantage' of a third party.[3]

Secondly, legal representation for an employee may be desirable where the employee's acts and omissions determine the criminal or regulatory liability of the corporate, for example where the employee is the 'controlling mind' of the corporate or an 'associated person' for the purposes of the Bribery Act 2010.[4] In these circumstances, the corporate may consider that legal advice will enable the employee to render a more reliable account in an interview – an outcome that furthers the corporate's interests in helping it more accurately to assess its own exposure to criminal or regulatory liability.

15.2.2 The role of the employee's lawyer prior to the interview

While the lawyer will always owe professional obligations to the client (i.e., the employee), the corporate may require the employee to agree to the lawyer acting on restricted terms. Such terms may define the scope of the lawyer's work and outline circumstances in which the lawyer's fees will not be paid or can be clawed back from the employee (e.g., if the employee becomes a whistleblower or is charged with a criminal offence). There may be other terms dictated by the corporate's insurers. However, nothing in such terms can derogate from the lawyer's professional ethical duty to act in the employee's best interests.[5]

It is not uncommon for a single lawyer (or law firm) to be asked to act for a number of employees all of whom will be interviewed in the internal investigation. Whether this is permissible is purely a question of professional ethics.[6]

While the employee's lawyer must be independent from those conducting the investigation, it is nearly always beneficial for the employee's lawyer to form a constructive relationship with the corporate's lawyers. This relationship should enable the employee's lawyer to understand the allegations being investigated, the employee's perceived role in relation to the allegations, and whether the corporate has reported the allegations to a law enforcement body. The lawyer should seek comprehensive disclosure prior to the interview of all documents the employee

3 Outcome 11.1 of the SRA Solicitors Code of Conduct. However, whether this outcome is likely to be breached in a corporate internal investigation has not been explored in any case law, and will depend on precisely how the interview is conducted.

4 *Tesco Supermarkets Ltd v. Nattrass* [1972] AC 153; sections 7 and 8 Bribery Act 2010.

5 Fundamental Principle 4, SRA Code of Conduct.

6 See Chapter 3, SRA Code of Conduct: the solicitor proposing to act for two or more witnesses must be satisfied there is no conflict between them, or no substantial risk of a conflict arising in future, unless specified appropriate safeguards are observed.

will be asked about and ensure that the employee has sufficient preparation time for the interview.

Clearly the employee's lawyer needs competence in the areas of law relevant to the allegations being investigated (e.g., bribery or the Financial Conduct Authority's (FCA) Senior Managers Regime). This competence will enable the lawyer to pre-empt the questions that are likely to be asked in the interview, to take meaningful instructions from the employee, to structure those instructions in a logical fashion, and to assess how well the employee would perform in the interview. This may require separate advice on employment law as well as advice from other jurisdictions if the allegations are international in nature or the corporate has self-reported to overseas law enforcement bodies.

The work performed by the employee's lawyer should lead to two fundamental tactical decisions. First, is it in the employee's best interests to attend the interview? Second, if the employee attends the interview, how should the questions be answered to advance his or her best interests?

Advising the employee whether to attend the interview 15.2.3

In most investigations, employees are told that they have a duty to co-operate with the investigation under their employment contract. Failing to attend the interview will ordinarily lead to the employee being suspended or dismissed. However, this outcome should never be the sole or even the primary factor to consider when advising an employee. Of equal or greater importance is the impact of the interview on any existing or future legal proceedings involving the employee.

The employee's duty to co-operate with the investigation is not akin to a statutory compulsion.[7] Equally, however, employees cannot sensibly attend the interview and then elect not to answer certain questions on the basis that they will incriminate themselves. Electing to answer some questions but not others is overwhelmingly likely to lead to the same result as refusing to attend the interview, namely suspension or summary dismissal.

If by co-operating and answering all questions the employee self-incriminates or admits to regulatory breaches, the interview is unlikely to serve his or her best interests. Not only is the employee likely to be dismissed or suspended given the nature of the admissions (the same outcome that would have occurred had he or she refused to attend the interview), but the corporate will obtain a damaging interview record which could be handed over, and used, in a law enforcement investigation. While the recent Court of Appeal judgment in *Director of the SFO v. ENRC*[8] clarifies the circumstances in which an interview record may be protected by litigation privilege, the corporate may choose to waive privilege as a hallmark of its co-operation. The interviewee must therefore be advised that he or she should only proceed with the interview if prepared to accept the real risk that a law enforcement body will ultimately review an audio recording or transcript of

7 It is merely a breach of a private employment contract and carries no statutory penalty.

8 [2018] EWHC 2006.

it, and potentially make important decisions about his or her status in any future criminal or regulatory investigation based on the answers given in the interview.

Whether the record of an interview in an internal investigation constitutes admissible evidence against the employee in legal proceedings has not been explored in any case law. However, there are analogous cases which suggest that, as long as warnings akin to *Upjohn* warnings are delivered at the commencement of the interview, the interview record would probably be admissible in criminal proceedings.[9]

Given that the interview record could be admissible against the employee, the employee's lawyer needs to balance the risk of dismissal or suspension against the risk of increasing the employee's exposure to personal liability in criminal and regulatory proceedings. If the employee is able to deliver a credible account without self-incrimination or admitting regulatory breaches, it will ordinarily serve his or her interests to attend the interview. Equally, there are circumstances in which employees will be advised to attend the interview even though they will admit criminal or regulatory offences, for example, the employee was junior, the offending is relatively trivial, and the employee wishes to be able to say, in any subsequent legal proceedings, that he or she gave the employer an explanation consistent with what he or she now asserts to the law enforcement body. However, if the employee is likely to admit serious offences in the interview, then attending the interview simply to advance mitigation is unlikely to be advisable.

See Chapter 13 on employee rights

15.2.4 The role of the lawyer in the interview

An employee attending the interview will typically be advised that, to advance his or her best interests, answers should be concise, contain no speculation and provide no extraneous detail beyond that required by the particular question. Ideally, this process occurs organically and the lawyer does not need to intervene during the interview. Nonetheless, the lawyer's presence is important, and interventions may become necessary, so as to ensure that:

- the employee is asked questions that are clear and fair;
- the employee is given an adequate opportunity to answer the questions without interruption, intimidation or improper pressure;
- the interviewers do not misconstrue any answers given by the employee;
- the employee does not inadvertently waive privilege over advice;
- the employee can take advice on an ongoing basis about issues that arise during the interview or previously undisclosed documents which he or she is asked to comment on;
- an accurate record is kept of the questions and answers; and
- the employee raises all material facts, defences and mitigation identified during the preparatory work conducted with the lawyer.

See Chapter 7 on witness interviews

9 *R v. Twaites and Brown* (1991) 92 Cr App R 106 CA; *R v. Smith* [1994] 1 WLR 1396; *R v. Welcher* [2007] Crim LR 804 CA.

Interviews of witnesses in law enforcement investigations 15.3

Law enforcement investigations are conducted under distinct statutory regimes, depending on the nature of the conduct under investigation and the agency conducting it.[10] However, in general terms, there are two types of witness interviews: interviews conducted voluntarily and interviews conducted compulsorily.

Voluntary interviews 15.3.1

The majority of interviews are conducted without the witness being subject to legal compulsion. In other words, the witness is interviewed as a volunteer. While being interviewed voluntarily may seem attractive in that it suggests a co-operative attitude toward law enforcement, the record of the voluntary interview (including any admissions made by the witness) could be used in evidence against the witness in subsequent legal proceedings. In criminal proceedings, this risk increases if the witness has received legal advice prior to the interview, because it becomes less likely that a court would use its discretionary power to exclude the interview.[11]

If there is a risk, however remote, that the witness will self-incriminate in the interview, it is unlikely to be in the witness's interests to attend voluntarily. In these circumstances, being compelled to attend the interview is likely to be advantageous.

Compulsory interviews 15.3.2

Where a witness owes a duty of confidentiality to another party concerning the subject of the investigation, or is concerned about the potential use of the interview record against him or her in subsequent proceedings, the witness will ordinarily refuse to attend the interview voluntarily. In some circumstances, the witness can be compelled to attend and answer questions under statutory powers available to all major investigators, including HM Revenue and Customs, the FCA, the Serious Fraud Office (SFO) and the police.[12] Where this compulsory power is used, the witness is protected from civil suit for breach of confidence. Moreover, the answers given cannot be used in evidence in criminal proceedings against the witness – an important protection that is not available in a voluntary interview.

There are two exceptions to this latter protection: first, where criminal proceedings are brought in respect of false or misleading statements made during the course of the interview; second, where the witness, who later becomes a defendant, advances a different version of events in subsequent proceedings.

The role of the lawyer and the reasons for intervening in compulsory interviews are similar to those in the interview of an employee in a corporate internal investigation.

See Section 15.2.4

10 For example, under section 1 of the Criminal Justice Act 1987 the SFO has a mandate to investigate serious or complex fraud; the FCA's statutory objectives are set out in the Financial Services and Markets Act 2000.

11 Section 78 of the Police and Criminal Evidence Act 1984.

12 See, for example, section 2 Criminal Justice Act 1987; section 62 Serious Organised Crime and Police Act 2005; section 165 Financial Services and Markets Act 2000.

15.3.3 Right to legal representation in a compulsory interview

There is no absolute right to a lawyer in a compelled interview, although usually a lawyer will be allowed to attend. In the context of compelled interviews with the SFO under section 2 of the Criminal Justice Act 1987, this principle was confirmed in *R v. Lord* and others.[13] In this case the SFO challenged a witness's choice of lawyer on the basis that it was the same lawyer that represented a corporate suspect in the same investigation. The SFO refused to permit the lawyer's attendance at an interview and the witness sought relief by way of judicial review of the SFO's decision. Permission for the judicial review was not granted and the Administrative Court upheld the SFO's decision to exclude the lawyer.

The SFO's response to this case was to withdraw its existing guidance on section 2 interviews and issue further guidance in June 2016.[14] This guidance creates inroads into the right to legal representation that go far beyond the factual scenario examined in *Lord*. Under the guidance, witnesses are reminded that they may consult a lawyer before and after an interview, but a request for representation by a lawyer during an interview will only be granted if, *inter alia*, the following conditions are met:

- a written request is provided in a prescribed period prior to the interview;
- the reasons that a lawyer is requested are set out;
- the lawyer agrees to undertake to a list of restrictions generally aimed at ensuring that information imparted or documents provided by the SFO remain confidential;
- the lawyer undertakes not to act for a suspect in the investigation; and
- the lawyer agrees to provide 'legal advice and essential assistance and otherwise not interrupt the free flow of truthful information which the interviewee, by law, is required to give'.

Despite these attempts to restrict a lawyer's role during the interview, it is important for a lawyer always to act in the best interests of the witness and in accordance with his or her professional obligations. The guidance was amended in February 2019 to allow an additional legal representative to attend the interview for the sole purpose of taking notes. (The original guidance had only permitted one lawyer to attend in most cases.)

The Law Society has issued a practice note that is essential reading for those advising the recipient of a section 2 notice.[15]

Any undertaking requested should be carefully considered. The Law Society practice note advises as follows: 'You should consider whether it is appropriate and necessary to agree the undertakings sought by the SFO on a case-by-case basis.

13 *R v. Lord and others* [2015] EWHC 865 (Admin).

14 https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/codes-and-protocols/.

15 https://www.lawsociety.org.uk/support-services/advice/practice-notes/representing-clients-at-section-2-cja-interviews/#cp21.

You should carefully consider the implication of agreeing to any undertaking and, if necessary, seek to amend the terms of the undertaking before agreeing it.'[16]

By way of example:

- Has sufficient information been provided to enable the lawyer to undertake whether he or she acts for another suspect?
- Do the undertakings on confidentiality relate to documents that are actually confidential (i.e., if the witness has obtained them from another source, this undertaking should be drafted to exclude such items)?
- Are the undertakings relating to the provision and retention of pre-interview disclosure practicable?

In respect of the conduct of the interview, the lawyer must give advice that the SFO may consider conflicts with the 'free flow of truthful information', for example:

- The lawyer must also ensure that the interview is conducted within the parameters of the section 2 power.
- The lawyer must ensure that the SFO respects the statutory exception to its compulsory power, such as a refusal to answer questions that are properly the subject of legal professional privilege.[17]
- The lawyer must ensure that the witness is able to deal with the interview properly: the lawyer must ensure that answers given by the witness are not misconstrued, that the witness has sufficient time to consider the documents put to him or her, etc.

Confidentiality of the interview 15.3.4

At the conclusion of an interview with a witness (and some interviews with suspects), the investigator will often inform the witness that they consider the interview to be confidential and that the witness should not discuss it with anyone other than their legal adviser. There is no legal force in these statements. In *Lord*, for example, the court confirmed that there is no obvious bar to an interviewee discussing their interview as they wished.[18] Indeed, there may be good reason for a witness (or his or her lawyer) to discuss what was learned in an investigator's interview with others; careful thought should therefore be given to whether this would be in the witness's best interests. The only exception to this is where the investigation is a money laundering investigation, in which case thought should be given to whether the prohibition on tipping off set out in section 333 of the Proceeds of Crime Act 2002 applies.

16 Paragraph 2.2 of the Law Society's practice note.

17 Section 2(9) Criminal Justice Act 1987. Legal professional privilege may be claimed over any communication between a client and their lawyer seeking or giving legal advice and over communications between a lawyer and a third party if litigation was in contemplation and the document or communication was created for the dominant purpose of litigation.

18 *R v. Lord and others*, paragraph 21.

15.4 Interviews of suspects in law enforcement investigations

15.4.1 The caution

Law enforcement interviews of suspects are conducted in accordance with the protections set out in the Codes of Practice (PACE Codes) issued pursuant to section 66 of the Police and Criminal Evidence Act 1984 (PACE). Among the most important of these protections is the caution administered to a suspect at the start of an interview.

An investigator must caution a person if there are 'reasonable, objective grounds for suspicion, based on known facts or information which are relevant to the likelihood the offence has been committed and the person to be questioned committed it'.[19] The failure to administer a caution may render the interview record inadmissible in subsequent criminal proceedings.

The caution is as follows:

> *You do not have to say anything. But it may harm your defence if you do not mention when questioned something which you later rely on in Court. Anything you do say may be given in evidence.*[20]

The caution confers on the suspect a right to silence. It also reminds the suspect that if he or she chooses to answer questions, the answers will be admissible in evidence against the suspect at any criminal trial. Finally, the caution alerts the suspect to a rule called the adverse inference. This rule means that, if the suspect fails to mention a fact that in the circumstances existing at the time could reasonably have been mentioned at the interview and later relies on that fact in his or her defence, there is a risk that the trial judge directs the jury that they may draw an adverse inference against the suspect.[21] The jury could draw an adverse inference, for example, if they found that the reason that no answer was given was because there was no good or true answer that would stand up to scrutiny, or if they found that any subsequent fact raised in the defence could be fabricated.

Jurors may not be asked about their deliberations and so the impact of a judicial invitation to draw an adverse inference is not known. Nonetheless, it is believed that jurors do not always draw an inference even when invited to do so.

15.4.2 Deciding on the suspect's approach

The single most important decision taken by a lawyer representing a suspect in an interview under caution is whether to answer questions, exercise the right to silence or read from a prepared statement. This decision is rarely straightforward; care must be taken to protect the suspect from a variety of risks, including the risk of making damaging admissions, the risk of being ambushed by previously

19 See Note 10A to paragraph 10.1 of Code C of the PACE Codes.

20 *per* PACE Code C, paragraph 10.5.

21 Section 34(1) and (2) Criminal Justice and Public Order Act 1994.

undisclosed documents and the risk of an adverse inference being drawn in any future trial.

To advise on this decision, the lawyer should seek pre-interview disclosure from the investigator, namely an explanation of the evidential basis of the allegations against the suspect. There is no legal requirement to provide pre-interview disclosure, although case law suggests that where none is given, disclosure is very limited or what is given is misleading, the court may decline to draw an adverse inference or may even exclude the interview from evidence.[22] In practice, most investigators will provide some pre-interview disclosure in an attempt to prevent these outcomes. If the disclosure is limited, for example if it contains a summary of facts with no contemporaneous documents, the lawyer should ask a series of questions to establish what evidence has been collected in the course of the investigation and seek sight of any document that will be put to the suspect in the interview. A note should be taken of these discussions so that it can be used in any subsequent application for exclusion of evidence or objection to an adverse inference.

If thorough disclosure is provided, a full comment interview may add credibility to a defence advanced at trial or give the investigator reasons to re-evaluate the factual basis of his or her suspicions. However, if disclosure is inadequate, answering questions may simply provide an account that is inconsistent with material already gathered by the investigator (and that may be deployed by the investigator during the interview to discredit the suspect's account). Moreover, answering questions without fully understanding the basis of the allegations may simply extend the scope of the investigation into new, problematic areas.

In complex financial crime cases, reading from a prepared statement may often be preferable to a suspect answering questions or exercising the right to silence. An effective prepared statement will set out the salient points in the suspect's defence in a structured format and guard against the risk of the adverse inference being drawn. However, there is always a risk in relying on these statements if disclosure is inadequate, such that the statement could be undermined at a later stage of the investigation or omit facts that could have reasonably been mentioned in interview. Practices vary as to whether such statements should be read out at the beginning or end of the interview.

Lawyers advising a suspect should ask themselves two questions. First, are there factors that may suggest the suspect is not able to provide a full and clear account of the conduct? Secondly, are there tactical reasons to adopt a certain approach? Some of the factors that feed into these questions are as follows:

- there are no facts on which the suspect will rely in his or her defence;
- pre-interview disclosure is so limited that it is not possible properly to evaluate and advise on the case against the suspect;

22 *R v. Mason* [1987] 3 All ER 481.

- limited disclosure may indicate that the investigator's case is weak and there is a risk that the suspect would make admissions that may strengthen the case or lead to new lines of enquiry;
- the disclosure, however briefly put, reveals the type of case that calls for a defence to be put in evidence at an early stage;
- the case disclosed is not based on admissible evidence;
- the conduct under investigation is historic or complex, such that inadequate time or disclosure has been provided to prepare effectively (this may not necessarily be the investigator's strategic decision but because evidence is still being obtained);
- the lawyer knows or suspects that the investigator plans to provide documents in the course of the interview that have not been shown to the lawyer in advance; and
- the suspect is by reason of illness, cognitive impairment, drink or drugs, fatigue or other mental state not able to provide an accurate account or take advice on board.[23]

15.4.3 The lawyer's role in the interview

The lawyer's role in an interview of a suspect is similar to the roles described above when acting for employees in corporate internal investigations or for witnesses in law enforcement investigations. However, there are additional considerations when acting for a suspect. For example, in some circumstances, he or she should be warned not to accuse others of lying or other reprehensible behaviour, as to do so will automatically risk their own 'bad character' (which includes non-conviction material such as disciplinary matters) being admitted in evidence.[24]

23 If any of these conditions are apparent, the suspect is likely to be unfit to be interviewed and medical advice should be obtained.

24 Under section 101(1)(g) of the Criminal Justice Act 2003.

16

Representing Individuals in Interviews: The US Perspective

John M Hillebrecht, Lisa Tenorio-Kutzkey and Eric Christofferson[1]

Introduction 16.1

When representing individuals in investigations, determining whether to consent to an interview and any interview itself can be pivotal. The following sets forth some potential pitfalls and suggests certain best practices.

Kind and scope of representation 16.2

Even leaving aside the multifarious sorts of industries and issues that can be relevant to the representation of an individual, there are various kinds of representations, presenting different types of challenges.

Representing current or former employees 16.2.1

Most typically in sophisticated white-collar matters, a company is either conducting an internal investigation into suspected misconduct or responding to a government investigation (regulatory or criminal, or both) of similar misconduct. The former often morphs into the latter, one way or the other. In those contexts, the individual client is usually a current or former employee or board member. Inevitably, the individual's relationship with the company is crucial, and can materially impact (for good or ill) counsel's approach to the interview. At the most basic level, the company may or may not have an obligation to advance reasonable legal fees and expenses to the client.[2] Even in the absence of a contractual or other obligation, the company will sometimes agree (or be persuaded) to do so. In either scenario, the company might impose a cap or other conditions on payments. In any event, there are significant advantages to the client establishing a co-operative

See Chapter 4 on self-reporting to authorities and Chapter 20 on whistleblowers

1 John M Hillebrecht, Lisa Tenorio-Kutzkey and Eric Christofferson are partners at DLA Piper.

2 See, e.g., 8 Del. C. § 145 (discussing advancement).

and cordial relationship with the company (including, at minimum, access to documents and other information) – although this is not always possible.

16.2.2 Pool counsel

At times, largely for reasons of efficiency and economy, the client may be one of multiple individuals a single lawyer concurrently represent as a 'pool' of clients who are witnesses or potential witnesses in the same investigation – subject to the ethical rules governing conflicts of interest and confidentiality.[3] This usually occurs where the members of the pool are viewed at that time as less culpable and whose interests are thought to be aligned. Such an arrangement presents obvious advantages to each individual. Pool counsel, by definition, obtains a broader perspective and usually has access to more documents than he or she would otherwise, has the benefit of each client's recollection, and can use insights gleaned from the first client's interview or interviews to prepare for subsequent client interviews. To be clear, it is usually best practice not to 'cross-pollinate' clients (by, for example, telling one client what another said about a particular issue), but pool counsel can appropriately use such information to formulate questions and strategies. Before agreeing to represent multiple individuals, counsel must take substantial steps to ensure that there are no conflicts, document the risk of future conflicts and the waiver of any future conflicts in appropriate engagement letters, and remain hyper-vigilant for developing conflicts.[4] The authors recently experienced a situation in which it emerged – a year into representing a pool of individuals – that one client had negative information about a second client (information both had concealed), leading to significant issues during fraught negotiations with the government regarding one of the two clients. Only the existence of an appropriate engagement letter forestalled more serious problems.

16.2.3 Joint defence agreements

Although 'entering into a joint defense agreement is often, indeed generally, beneficial to its participants, like skating on thin ice, dangers lurk below the surface'.[5] These dangers are illustrated by court rulings disqualifying counsel based on a joint defence agreement, precluding counsel from cross-examining a defector who becomes a cooperating witness, and holding that communications thought to be protected by a joint defence agreement were not in fact privileged.[6] Most of these risks can be mitigated substantially if counsel for the participants consider, discuss and record in some fashion the parameters of their agreement, including the

3 See generally Association of the Bar of the City of New York Committee on Professional Ethics, Formal Opinion 2019-4: *Representing Multiple Individuals in the Context of a Governmental or Internal Investigation (Opinion 2019-4).*

4 See generally *Opinion 2019-4*.

5 *United States v. LeCroy,* 348 F. Supp. 2d 375, 387 (E.D. Pa. 2004), as amended on reconsideration (10 January 2005).

6 See generally *United States v. Hatfield*, 2009 WL 3806300 (E.D.N.Y. 2009).

consequences of one or more participants withdrawing from the agreement.[7] On more than one occasion when the authors represented individuals, we received a voluminous quantity of documents from the clients' former employers, all Bates-numbered to the effect that they were produced pursuant to a joint defence agreement, when there had been no discussion about any such agreement. The tendency of many practitioners to prefer informal joint defence agreements with no specific clarity or agreement on the consequences of withdrawal is puzzling, and the consequences can be severe.[8]

In some jurisdictions, including the Southern District of New York (SDNY),[9] practitioners often prefer to use verbal joint defence agreements. While the agreement need not be recorded in writing, there are numerous advantages to doing so. Although courts may find the existence of a joint defence agreement, despite the agreement being purely verbal, the existence of a written document obviates this inquiry. In a December 2018 decision, a judge in the SDNY held that a former employee failed to establish a common interest agreement with his former employer – even though the individual's lawyer emailed company counsel a draft document with the subject line 'Common Interest Privilege Document', specifically noting that the draft document was being shared 'pursuant to our common interest', without any objection or clarification from company counsel.[10] This underscores the importance of documenting explicitly the existence of such an agreement.

Companies under investigation will at times enter into a joint defence agreement with employees or, more commonly, former employees. We have seen such agreements stating that information disclosed to the company will not be disclosed to the government or third parties. This practice is problematic where a company would prefer to disclose illegal or wrongful conduct to the government and minimise its exposure by obtaining co-operation credit, or where the company operates in a regulated industry that imposes a legal obligation on the company to disclose wrongdoing. As a result, counsel for a corporation typically include language in the joint defence agreement that explicitly authorises the corporation to disclose joint defence materials (or a subset of them) at its sole discretion. This kind of joint defence agreement is little more than a glorified *Upjohn* warning.[11] In representing entities, the authors have in the past used joint defence agreements that protect most joint defence materials – strategy discussions, draft work

See Chapter 4 on self-reporting to authorities

7 Unfortunately, far too often the sum total of counsels' 'discussion' along these lines can be summarised as 'This is a joint defence meeting, right?'.

8 See John M Hillebrecht and Jessica Masella, 'Understanding Joint Defense Agreements: The Implications for White-Collar Defendants in the Second Circuit,' *New York L. J.* (25 January 2019).

9 The Southern District of New York (SDNY), centred on New York City, is home to many of the US Department of Justice's (DOJ) most significant international prosecutions and one of its largest US Attorneys' Offices.

10 *SEC v. Rashid*, 17-cv-8223 (PKC) (S.D.N.Y. 13 December 2018).

11 See generally *Upjohn Co. v. United States*, 449 U.S. 383 (1981). See also Chapter 8 on witness interviews.

product, updates on interactions with the government – but specifically carve out 'historical' interviews of the individual, which are governed by a standard *Upjohn* warning. As a practical matter, however, whatever the form of the joint defence agreement, an individual may have little choice but to agree so as to obtain information (including documents) necessary to present a defence.

16.3 Whether to be interviewed

16.3.1 Internal investigation

At times a client faces real risk in consenting to an interview by the company. Admitting misconduct, even mere violations of company policy well short of criminal violations, can result in discipline, termination and severe financial consequences. Also, one must assume (and advise one's client to assume) that the company will disclose its version of the interview to the government. Hence, before consenting to an interview, it is crucial to understand the facts (including the documents, the context of the transaction or trading strategy etc., and the client's version of events), as well as the views of company counsel (to the extent they can be elicited). That said, the client often faces a Hobson's choice. The company's advancement of fees (which the client may regard as crucial) may well be conditioned on co-operation and, more fundamentally, in the United States (as opposed to virtually all EU countries) an employer can generally fire an executive who refuses to be interviewed.[12] Even where there is some degree of risk, when the client wants to continue employment, protect his or her financial situation, or simply continue working for a different employer in the same regulated industry, the incentives to consent to an interview will be strong. Even leaving those concerns aside, failure to consent to an interview will almost certainly lead to a cessation of reciprocal co-operation from the company – halting the flow of documents and updates and putting an end to coordination. Obviously, there will be cases where the risks of a truthful interview are so palpable that, regardless of the consequences, declining to be interviewed is the only prudent choice. Similarly, many individual clients face close to no risk. The troublesome choices concern those clients who fall in between.

16.3.2 Government investigation

Consenting to a government interview obviously carries additional risks. Therefore, assessing the client's exposure in advance is even more crucial in this context. In addition to assessing the facts and documents, prudent counsel will seek the views of company counsel, speak to counsel for other potential witnesses (whom company counsel will usually identify), and if applicable review public record documents, related civil lawsuit filings and media reports (and, increasingly, blogs and other internet commentaries). Equally important are the views, if they can

12 See *Gilman v. Marsh & McLennan*, 826 F. 3d 69 (2d Cir. 2016); see also Michael D Hynes, Brett Ingerman, John M Hillebrecht, 'Second Circuit Affirms Employers' Right to Terminate Employees Who Fail to Cooperate With Internal Investigations,' *DLA Piper Client Alert* (1 July 2016), https://www.dlapiper.com/en/us/insights/publications/2016/06/second-circuit-affirms-employers/.

be obtained, of the government lawyers seeking the interview. The United States Department of Justice (DOJ) has a formal taxonomy between 'target', 'subject' and (less formally) witness.[13] Often, but not always, counsel representing an individual can at minimum get an Assistant US Attorney to answer a question regarding the client's formal status (although it is imperative that the client understand that the status can always shift). Other agencies – for example the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) – usually will not provide even such minimal information, but there are frequently exceptions.

Of course, even when contemplating a government interview there are often similar employment-related considerations – an obligation to co-operate to avoid a cut-off of legal fees, termination of employment, or even attempted clawbacks of vested bonuses, etc. And, again, certain executives in regulated industries (e.g., registered broker-dealers) can be easily placed between a rock and a hard place. Also, unlike company counsel, the government can always threaten to use grand jury or other subpoenas.[14]

See Chapter 14 on employee rights

Preparation for interview 16.4

For both internal and government interviews, the typical preparation is much the same. This is where having a good relationship with company counsel becomes so important. If company counsel has provided the key documents, identified counsel for other individuals and shared (within reason) the focus of the investigation (from the company's perspective or that of the government), counsel for the individual client will be well positioned to prepare the client for the interview. Conversely, if company counsel has not been co-operative, preparing the client becomes more difficult. Counsel should in any event push the interviewer (company counsel or the government) to identify in advance the topics to be covered and to share in advance the documents to be used during the interview. How much of this is actually made available varies enormously, based on a number of factors. Sometimes everything requested is supplied; sometimes next to nothing is forthcoming; but usually the requests are partially satisfied. As a very general observation, certain government entities (e.g., the CFTC) are usually more forthcoming than others (e.g., the DOJ). But in any event, there is no harm in asking, if necessary repeatedly.

Even where company counsel shares 'all' the key documents, more often than not crucial – unfortunately, at times the most crucial – documents are omitted. Often, company counsel will produce to the individual client's counsel 'all' the

13 See generally Justice Manual § 9-11.151.

14 The foregoing discussion focuses on the US perspective for individuals located in the United States. For clients located abroad, the calculus may differ in nuanced ways. Among other things, the ability of companies to compel co-operation is markedly less in other jurisdictions (e.g., the European Union) and the ability of US agencies to effectively subpoena persons abroad (through mutual legal assistance treaties or otherwise) is much more limited. (See Chapter 11 on production of information to authorities and Chapter 28 on extraterritoriality.)

documents the client saw in real time that have been produced to the government and a separate subset of the most important documents. One should never rely on the company's selection. Instead, counsel should run targeted searches on the broader universe of documents. Even then, counsel must bear in mind that that universe (1) obviously does not include documents produced by other entities (which are frequently encountered for the first time when the client is confronted with them during a government interview or SEC testimony); (2) might not include all documents produced by the company; and (3) might also not include other documents (texts, instant messages, WhatsApp messages, private emails, etc.) that may have escaped the company's net. In this regard, it is important to remember to ask the individual client early on whether he or she has access to any pertinent documents or communications (including texts and other messages on a work or personal cellphone or other device).

Recognising these limitations and risks, the documents are typically an essential part of preparing for an interview. It is often helpful to conduct a preliminary debriefing of the client without delving too deeply into large numbers of documents. Then, armed with the context and insights provided by that preliminary conversation, counsel typically spends substantial time alone with the documents – reviewing, highlighting, annotating, cross-referencing and generally striving to internalise the pertinent documents. While the initial cut of such a review will typically be performed by junior lawyers on whatever electronic document review platform they favour, depending on volume and lawyer predilections it is often easier for the senior lawyer to review and annotate the most significant documents in hard copy, in binders, with highlighters and post-it flags. Every lawyer's methodology will differ, but the point of the exercise should be a constant: identify those documents that are central to the narrative; flag the phrases, paragraphs and emoticons that will grab the attention of a prosecutor, regulator or company counsel; and put together a comprehensible chronology.

A written chronology is often a helpful vehicle to identify salient points and, at a minimum, provides a helpful tool to refresh recollections. During the life of many investigations, there will often be dormant periods where months go by without much or any activity. When the SEC subsequently calls, having a detailed chronology document to reference is a good way to get back up to speed quickly. In building out a chronology, the precise time of day a message was sent is often overlooked. At times, such details support inferences, good or bad, and the reviewing attorneys must be sensitive to that.

Once counsel has done their level best to carefully scrutinise and organise all the relevant documents available, they should be reviewed in detail with the client. In some cases, there are multiple discrete issues (e.g., a revenue-recognition matter raising different issues for a company's different customers) and some where there is really a single issue (e.g., an insider trading investigation focused on a single trade by one trading desk). In the former situation, one would generally break up the documents by issue, whereas, in the latter, chronological order usually makes most sense. Even in a case involving multiple different issues, it is important not to be too rigidly siloed. Often, the fact that an email or text regarding one subject

was sent shortly before a seemingly-unrelated message regarding another can loom large as to the client's state of mind or other important issues.[15]

After the documents are reviewed and organised, the client should be walked through them. It often makes sense to provide the client with a collection of the pertinent documents in advance. (On occasion, company counsel will put restrictions on the use of the documents it has provided, including precluding the individual client from reviewing the documents outside the presence of counsel. Where required, clients can review the documents with a junior lawyer or paralegal in the room.)

An important goal of such preparation is to refresh the client's recollection as to documents and events that often are from years earlier. But almost invariably, portions of some documents will suggest improper conduct as to which the client must be prepared (if possible) to offer a cogent explanation. Sometimes what looks bad to an outside observer turns out to be perfectly proper when put in the context of the industry or transaction at issue. Sometimes what looks bad is truly a joke or sarcasm. And sometimes what looks bad is, frankly, bad.

In identifying potentially problematic aspects of documents, it is important for counsel to put his or her prosecutor's cap on and cast a jaundiced eye on the documents. To the extent possible, it is also important to speak with counsel for other individuals who received the same document to try to elicit the other individuals' understanding of it and the views of the government or company counsel (to the extent there have already been interviews).

One strategic issue that sometimes arises has to do with whether ignorance is bliss. There may be times when *not* refreshing the client's recollection or, more frequently, not educating him or her about an issue (e.g., an accounting rule, a regulatory requirement) makes sense.

Once the client is as well versed in the documents and other information at issue as can be expected, it is sometimes a good idea to pressure-test his or her explanations and recollection by conducting what is tantamount to a mock cross-examination. This enables the client to become familiar with limiting answers to what he or she knows and remembers, to avoid speculation or characterisations, and to make what was known and understood at the time as opposed to now (following focused review of documents and awareness of the investigation).

Procedures for government interview 16.5

After tentatively deciding to consent to a government interview, it may be prudent to preface the actual client interview with an attorney proffer. These are more commonly used with some government agencies than others. For example, they are commonly welcomed by the Antitrust Division of the DOJ. Although practices differ among jurisdictions and government regulators, typically counsel

15 At least some of the authors have had the unpleasant experience of realising such a connection only in the middle of a DOJ interview, a situation that should be avoided at all costs.

would prepare a detailed outline of a proffer, vetted and approved by the client, and stick to it while presenting to the government.

Counsel should inform the government that the proffer is hypothetical but that the information is what counsel expects the client would say. Counsel should then recount the information prepared in advance and typically not answer any questions the government asks with additional information not vetted with the client. The purpose of such a proffer is to gauge the government's view of the client's exposure. Typically, an attorney proffer is used in the context of DOJ criminal investigations where counsel believes the client is in some degree of jeopardy. Often the proffer will conclude with some version of: 'If the client tells you what counsel has just summarised, would you agree that a non-prosecution agreement would be proper?'[16]

Some years ago, such proffers were very common in criminal cases, particularly where counsel was seeking a co-operation agreement or non-prosecution agreement. Many US Attorney's Offices have in recent years taken the position that an attorney proffer is no different from a client proffer in that the attorney's statements are treated as statements of the client for purposes of the Jencks Act and therefore must be disclosed to defence counsel if the client becomes a government witness.[17] Accordingly, prosecutors have been more reticent about agreeing to attorney proffers.

Assuming the decision is made (either given positive feedback from an attorney proffer or otherwise) to go forward with the government interview or proffer, a number of important preliminary matters must be resolved in advance. Perhaps most importantly, counsel must clearly explain to the client – and document – all the risks and benefits of making a proffer, and that it would be voluntary and the Fifth Amendment generally precludes anything but a voluntary proffer.[18] Equally fundamentally, counsel must confirm which agencies, and what offices from each agency, will be attending; not only may the risk profiles differ, but each agency may have different ground rules, including different proffer agreements or no proffer agreements at all.

Although, as discussed below, many proffer agreements today provide imperfect protections, they do provide some protection. Accordingly, one crucial requirement of any proffer agreement is a 'most-favoured nation' clause – a commitment from the government agency that it will not share the substance of any proffer with any other agency (foreign or domestic) not bound by the agreement. In this regard, the standard proffer agreement used by the SEC and the typical proffer agreement used by many US Attorney's offices provides that they will not

16 Some jurisdictions (such as SDNY) often use non-prosecution agreements for individuals, while others (such as the District of Massachusetts) never do.

17 18 U.S.C. § (Jencks Act); see generally *United States v. Triumph Capital Group*, 544 F. 3d 149, 161 to 165 (2d Cir. 2008) (reversing conviction because government failed to produce government notes of an attorney proffer).

18 Curiously, if a proffer does not produce the desired result, some clients have a tendency to forget that the risks were clearly explained to them.

share the proffer with another enforcement agency unless that agency agrees to be bound by the terms of the proffer agreement.

The most common types of proffer agreements (such as those used by the SEC and most US Attorney's offices, including the SDNY) have become longer and more complicated over the years. But the basic minimal protection provided by such an agreement has long ensured that the government cannot use the words the client says in the proffer as direct evidence in seeking an indictment (or filing a civil complaint) or as proof in the government's case-in-chief. This is a material benefit to the client. Absent the proffer agreement (or the agreement by the government to take a proffer subject to the plea-negotiation protections of Federal Rule of Criminal Procedure 11 or Evidence Rule 410 – which the authors have never known to have happened), the government could simply treat the client's statements as a confession and use them accordingly.

But the exceptions that have been added to these typical proffer agreements over the years, largely supported by the courts, have denuded this basic protection of much of its robustness. Indeed, many savvy practitioners as a matter of near uniform policy will virtually never advise their clients to proffer. One thing is patently clear: if the strategy of consenting to a proffer does not succeed and the client ends up getting indicted, the fact that the client proffered will almost invariably put the client in a worse position.

Assuming the client told a version of his or her state of mind or other issues inconsistent with the government's view of those matters, the typical proffer agreement permits the government to prosecute the client for false statements – basically, for denying culpability or contradicting what others say.[19]

More commonly, the government uses various terms of the typical proffer agreement to essentially eviscerate the ability a defendant who has proffered to defend himself or herself. Years ago, the typical agreement allowed the government to impeach a defendant who takes the stand with arguably inconsistent statements from the proffer session. That baseline exception has been expanded throughout the years. It is now broadly accepted that if defence counsel makes an argument in opening statement arguably contrary to the proffer statements or cross-examines government witnesses in the wrong way, the government can use the proffer statements – an obviously devastating piece of evidence.[20] Even something as simple as offering documentary evidence tending to show that the defendant was not at the scene of the crime can have the same effect.[21] In at least

19 See, e.g., *United States v. Percoco*, 16 Cr. 776 (VEC) (S.D.N.Y. 11 December 2017) (individuals who proffered exculpatory explanations during meeting with government after being 'told that they were "subjects" of the investigation', not 'targets', subsequently indicted for false statements.)

20 See generally *United States v. Barrow*, 400 F. 3d 109, 113 to 119 (2d Cir. 2005) (where proffer agreement stated that statements could be used 'as substantial evidence to rebut any evidence offered or elicited, or factual assertions made by' defence, assertion in opening that another person made certain specific narcotics sales opened the door to prosecution using proffer statements in case-in-chief which discussed drug dealing more broadly; 'proper rebuttal is not limited to direct contradiction').

21 See generally *United States v. Roberts*, 660 F. 3d 149 (2d Cir. 2011).

one case, *omissions* from a proffer statement were deemed admissible based on cross-examination of a government witness.[22]

So the risks of a proffer, and the loopholes in standard proffer agreements, are very substantial. Again, counsel must make a risk assessment, weigh the pros and cons, and explain all of this clearly to the client and document it.

Probably the last significant preliminary matter (other than pressing, yet again, for advance notice of the documents and topics the government expects to cover) is to determine in what fashion the government agency intends to record the interview. At least some government agencies (in our experience, often Inspectors General of various executive branch agencies) have a policy of seeking to audio-record voluntary interviews. Counsel and client should only consider consenting if the agency agrees to share the recording.

In the ordinary course (and certainly in the typical DOJ and SEC interviews), the government will have a designated note-taker (generally a law enforcement agent in a DOJ investigation) using a laptop or pen and paper. It is crucial that counsel for the client has a note-taker who has clear instructions as to what he or she should be doing. Unlike notes of a preparation session protected by attorney–client privilege, notes of a proffer to the government are protected only as work product. The note-taker in that context should strive to record all substance, even at times in 'Q and A' fashion and including interjections, objections, and clarifications by counsel for the client. While in the authors' experience it happens rarely, there are times when the government's notes as to a proffer are completely wrong on crucial issues (e.g., state of mind 'at the time' of the conduct in question) and the existence of painstakingly detailed notes proved to be an essential weapon in arguments with the DOJ and the SEC. Accurate, detailed note-taking is a must.

See Chapter 36 on privilege

Every proffer interview is different. Government lawyers are only human, so the approaches and temperaments of those lawyers run the gamut. Some ask almost entirely respectful open-ended questions. Some start an aggressive cross-examination shortly after initial introductions. Some are respectful and even-keeled but relentlessly ask the same exact question over and over again in an effort to get the client to shift his or her answer and adopt a specific formulation or term that is important to the prosecutor's theory. All of these happen – often during the same interview – because in a typical sophisticated white-collar matter, there can be two, three, four or more government lawyers asking questions. When this is the case, the individual client's lawyer must not be 'a potted plant'. The practitioner has a duty to stop a client answering unfair questions, to rephrase questions that are formulated in a misleading fashion, and to challenge the government lawyers when they misstate the client's earlier answers or misleadingly summarise documents or ask questions about one document while ignoring another equally relevant one (which counsel will hopefully know because he or she is conversant with all the documents that have been produced). A good proffer is

22 *United States v. Vella*, 2011 WL 652752 (3d Cir. 2011).

one where counsel largely stands mute. But one cannot be shy when shenanigans like those summarised above are playing out. To be clear: the government lawyers will not like it. They will accuse you of 'coaching' the client. They may ask you to step out of the conference room and tell you (in essence) to shut up. That is them doing their job. But you have to keep doing your job – respectfully, strategically and within reason. Counsel will, of course, have prepared the client for this potential dynamic.

Conclusion 16.6

Representing individuals in white-collar matters is always fraught with risk. The interview – whether by company counsel or the government – is a key step in any investigation, and one that typically crystallises the risks to the client. Advising a client on whether or not to consent to such an interview is thus something that must reflect your considered judgement. A well-prepared client, whose context you fully understand and whose documents you are confident have been reviewed, may materially advance his or her position by consenting to such an interview. But these risks should always be in the forefront of your mind.

17

Individuals in Cross-Border Investigations or Proceedings: The UK Perspective

Richard Sallybanks, Ami Amin and Jonathan Flynn[1]

17.1 Introduction

In any cross-border investigation, invariably suspects will either be located in different jurisdictions, or subject to investigation by authorities from different jurisdictions, or both.

This chapter looks at the key issues that can arise when acting for an individual who is present in the United Kingdom and subject to a criminal investigation or proceedings here or in one or more overseas jurisdictions.[2]

17.2 Cross-border co-operation

See Chapter 9 on co-operating with authorities

There are various ways in which the United Kingdom might co-operate with overseas agencies or regulators when investigating or prosecuting an individual, ranging from informal 'intelligence sharing' to mutual legal assistance (MLA).

In the United Kingdom, the framework governing MLA requests is contained, primarily, in the Crime (International Co-operation) Act 2003 (CICA), Part 1 of which deals with criminal cases. Under CICA, an MLA request can only be made if it appears to the investigating authority that an offence has been committed (or there are reasonable grounds to suspect that an offence has been committed), and proceedings have been initiated or an investigation has begun.[3] MLA requests

1 Richard Sallybanks is a partner, and Ami Amin and Jonathan Flynn are associates at BCL Solicitors LLP.

2 Whereas England and Wales have a common legal system, there are certain substantive and procedural differences in the Scottish and Northern Irish systems. This chapter focuses on the English and Welsh legal system.

3 Section 7, Crime (International Co-operation) Act 2003.

are made to the UK Central Authority (UKCA)[4] through a formal international letter of request, known as a *commission rogatoire* in civil law jurisdictions. The UK Home Office has published detailed guidance on how authorities outside the United Kingdom can make such requests.[5] MLA requests will only be considered appropriate, however, when the request is for evidence (and not intelligence).[6]

Where overseas police and other law enforcement agencies request assistance directly from a UK law enforcement agency, a formal MLA request is not required. A number of UK law enforcement agencies[7] can receive direct requests, and often this form of co-operation is governed by data sharing agreements or memoranda of understanding.

In some instances, cross-border co-operation may extend to the establishment of a joint investigation team (JIT) between investigating agencies in more than one country.[8] The establishment of a JIT is another means by which information or evidence gathered in one country can be shared with another without the need for MLA.

Practical issues 17.3

Asset freezing and restraint 17.3.1

During a cross-border investigation, an overseas authority may seek to freeze or restrain an individual's assets in the United Kingdom. The Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005 (the 2005 Order) sets out the provisions for the United Kingdom to respond to and co-operate with other countries in freezing and confiscating assets.[9] Under section 444(1)(a) of the Proceeds of Crime Act 2002 (POCA), property in the United Kingdom can be frozen in accordance with an external request relating to proceedings for the recovery of criminal proceeds.[10]

In the first instance, external requests will be addressed to the Secretary of State for the Home Department (SSHD), who will in turn refer the matter to the relevant UK authority.[11] The relevant authority will then apply to the Crown Court

4 The UKCA is the Home Office department responsible for receiving, acceding to and ensuring the execution of MLA requests in England, Wales and Northern Ireland. Her Majesty's Revenue and Customs (HMRC) is responsible for MLA requests in England, Wales and Northern Ireland relating to tax and fiscal customs matters. The Crown Office is responsible for MLA requests in Scotland, including devolved Scottish matters.

5 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf.

6 Section 7(2), Crime (International Co-operation) Act 2003.

7 These are: the UK Liaison Bureau at Europol via the National Crime Agency, Interpol via the National Crime Agency, UK Visas & Immigration; HMRC; Police Services; Financial Intelligence Units; Asset Recovery Offices.

8 Sections 103 and 104 of the Police Reform Act 2002.

9 The Order is made in exercise of the powers conferred under section 444 and 459(2) POCA.

10 An external request is a request by an overseas authority to prohibit dealing with property identified in the request. Section 447(1) POCA.

11 The relevant authority will be the Director of the National Crime Agency or the Director of Public Prosecutions and, in respect of offences involving serious or complex fraud, the Director of the

for the assets to be restrained. For the Crown Court to give effect to an external request: the property in England and Wales must be identified; a criminal investigation or proceedings relating to the relevant offence must have commenced in the requesting state; and there must be reasonable cause to believe that the alleged offender has benefited from his or her criminal conduct.[12] Furthermore, under section 447(8) of POCA, the criminal conduct must meet the dual criminality requirement, in that it must also amount to an offence in the United Kingdom, or would do so if it occurred there.

Where the Crown Court is satisfied that these conditions are met, it may make a restraint order prohibiting a person from dealing with the property identified in the external request, subject to certain exceptions.[13] A restraint order must be served on the suspect and any other person affected by it, and the UK courts will require confirmation this has been done. Failure to do so could result in the order being discharged.

Where a restraint order is obtained, it is likely that any banks or financial institutions to which the individual is connected will be served with a copy of the order in order to freeze any assets (ensuring that they remain available for confiscation).

The provisions of the 2005 Order correspond to provisions in Parts 2 to 4 and Part 5 of POCA (excluding Chapter 3), applicable to UK investigations. As with Parts 2 to 4 of POCA, section 444 enables restraint orders to be granted from the outset of a criminal investigation.

17.3.2 Account monitoring orders

CICA implements the 2001 Protocol to the Convention on Mutual Assistance in Criminal Matters (the 2001 Protocol), which creates obligations for participating countries to respond to requests from overseas authorities for assistance locating bank accounts or to provide banking information relating to criminal investigations.[14] Account monitoring orders under CICA only apply to an investigation by a 'participating country' into serious criminal conduct.[15]

Account monitoring procedures were first introduced in the United Kingdom under POCA. However, separate provisions have been created under CICA to ensure that the United Kingdom can meet the requirements of the 2001 Protocol, which has a wider scope than POCA.

Where the SSHD receives a request from the relevant overseas authority, he or she may direct a senior police officer to apply, or arrange for a constable to apply, for an account monitoring order.[16] A judge can make an account monitor-

Serious Fraud Office (article 6, the Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005).

12 Article 7, The Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005.

13 Ibid., article 8.

14 Sections 36 to 42, Crime (International Co-operation) Act 2003.

15 The request must be from an EU Member State, Iceland, Japan, Switzerland or the United States.

16 Section 35, Crime (International Co-operation) Act 2003. An account monitoring order is an order made by a judge to enable transactions on a particular account to be monitored for a specified period.

ing order where he or she is satisfied that there is an investigation into criminal conduct in the country in question and the order is sought for the purposes of that investigation.[17] Applications can be made, without notice, to a judge in chambers.[18] The court may discharge or vary an account monitoring order, but not on an application by the account holder.[19]

An account monitoring order can also be requested under Part 5 of the Proceeds of Crime (External Investigations) Order 2014 for the purposes of a criminal investigation[20] or criminal proceedings.[21] The request must demonstrate reasonable grounds for believing that the account information requested is of substantial value to the overseas investigation, and that it is in the public interest for it to be provided.[22]

Under POCA, account monitoring orders may be made for up to 90 days and the same restrictions apply to requests under the 2001 Protocol. Arrangements will be made between the relevant authorities case by case.[23]

Asset tracing 17.3.3

All asset tracing should be conducted via law enforcement co-operation through financial intelligence units. The United Kingdom has no central record for bank accounts. Therefore, any information should be sought via police co-operation before an MLA request is made.

In the United Kingdom, property or a sum of money is recoverable if it has been specified in an external order.[24] However, if the property (including money) specified in the external order has been disposed of, it is only recoverable if it is held by a person into whose hands it may be followed.[25]

Under the 2005 Order, any property deemed to represent the original recoverable property is also recoverable.[26] If a person disposes of recoverable property that represents the original property, the property may be followed into the hands of the person who obtains it (and it continues to represent the original property).[27]

17 Section 36, Crime (International Co-operation) Act 2003.
18 Ibid.
19 Ibid.
20 Provided that the investigation falls within a confiscation investigation or a civil recovery investigation.
21 Part 8, POCA.
22 Article 30, Proceeds of Crime (External Investigations) Order 2014.
23 Article 3(4) of the 2001 Protocol to the Convention on Mutual Assistance in Criminal Matters.
24 Article 202, the Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005.
25 Ibid.
26 Ibid., Article 203.
27 Ibid.

17.3.4 Confiscation and forfeiture

Under the 2005 Order, property within the United Kingdom may be subject to confiscation proceedings following the receipt of an external order.[28]

Upon receipt of an authenticated external order, the SSHD may refer it to the relevant UK authority to process.[29] Only the relevant Director (as defined in article 18 of the 2005 Order) may then make an application to the Crown Court to give effect to it.[30] The Crown Court must decide to give effect to an external order by registering it where certain conditions are met. Those conditions are that (1) the external order was made following a conviction of the person named in the order, and no appeal is outstanding, (2) the external order is in force and there is no appeal outstanding in respect of it, (3) giving effect to the order would not be incompatible with the Convention rights[31] of the individual concerned, and (4) the property is not subject to charges under the provisions set out in article 21(6) of the 2005 Order.[32]

Where the Crown Court decides to give effect to an external order, it must register it and provide for notice of the registration to be given to any person affected by it,[33] who may apply to vary the property to which it applies.[34]

Under article 26 of the 2005 Order, the amount ordered to be paid is due on the date notice is given to the affected person. The Crown Court has discretion to allow for more time to pay.[35] Where the external order specifies a sum of money in another currency, the sterling equivalent in accordance with the exchange rate prevailing at the end of the working day immediately preceding the day of registration of that order will be sought.[36]

17.3.5 Interviews

See Chapter 15 on representing individuals in interviews

An individual suspected of criminal activity who is resident or temporarily present in the United Kingdom and whom the UK authorities wish to question will be interviewed 'under caution'. This is usually done voluntarily unless it is

28 An external order is made by an overseas court where property is found, or believed to have been obtained, as a result of, or in connection with, criminal conduct. Section 447(2)(b) POCA.

29 The relevant authority will be the Director of the National Crime Agency or the Director of Public Prosecutions, and, in respect of offences involving serious or complex fraud, the Director of the Serious Fraud Office (article 18, the Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005).

30 Article 20, the Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005.

31 Rights under the European Convention on Human Rights.

32 The fourth condition is that the specified property must not be subject to a charge under: (a) section 9 of the Drug Trafficking Offences Act 1986(2); (b) section 78 of the Criminal Justice Act 1988(3); (c) article 14 of the Criminal Justice (Confiscation) (Northern Ireland) Order 1990(4); (d) section 27 of the Drug Trafficking Act 1994(5); (e) article 32 of the Proceeds of Crime (Northern Ireland) Order 1996(6) (article 21, the Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005).

33 Ibid., article 22.

34 Ibid., article 22.

35 Ibid., article 26.

36 Ibid., article 25.

considered necessary to arrest the individual and there are legitimate reasons for doing so, such as a reasonable belief that, unless placed under arrest, the suspect will abscond from the jurisdiction or will somehow attempt to improperly interfere with the investigation.[37]

Either way, the interview will be conducted in accordance with the procedures laid down in the Police and Criminal Evidence Act 1984 (PACE) and the accompanying Code C. The suspect has a number of rights, including the right to have a lawyer present.[38] A lawyer is defined as a UK solicitor holding a current practising certificate or an accredited or probationary representative.[39] This means that the suspect cannot be represented during the interview by an overseas lawyer. However, the suspect may have an approved interpreter present if he or she does not speak, or has only limited, English.[40]

The question of whether the interview is admissible in proceedings in any other jurisdiction will depend on the laws of that country. This means that, in cross-border investigations, serious consideration must be given by all the suspect's legal advisers prior to any interview in the United Kingdom as to whether his or her answers (or silence) may be admissible in any other investigating jurisdiction and, if so, the resulting potential benefits or disadvantages of the strategy adopted.

When a suspect is resident in the United Kingdom, but is wanted for questioning by an overseas authority, the individual (or his or her legal advisers) may be approached with a request that the suspect travel to the country of the requesting authority for interview voluntarily.

In the absence of any such request, or if it is refused, the requesting authority may be able to gain evidence from the suspect in the United Kingdom through MLA. In brief, an overseas authority can request that a statement be taken from the suspect on a voluntary basis. Alternatively, where the evidence needs to be taken on oath or where the suspect refuses to co-operate, the request can be for the suspect to be compelled to attend court for questioning.

Once before the court, the suspect can then be questioned under oath (although an oath need not be administered if this is allowed under the laws of the requesting state). The suspect retains the right against self-incrimination and may refuse to answer any question.

If a suspect consents to giving the overseas authority a statement voluntarily, or answers questions in court, this is likely to be admissible in any future proceedings in the requesting jurisdiction (subject to the applicable law in that jurisdiction). Again, the question of whether statements are also admissible in proceedings in any other jurisdiction will depend on local laws, and serious consideration must be given by all the suspect's lawyers of the implications.

37 Section 24 and Code G Police and Criminal Evidence Act 1984 (PACE).

38 Paragraph 6, Code C PACE.

39 Paragraph 6.12, Code C PACE.

40 Paragraph 13, Code C PACE.

Often the requesting state seeks to obtain evidence from an individual who is not a suspect, but who is a witness, in the investigation. In such situations, the same MLA procedures can be used to obtain evidence.

However, if it is believed that the non-suspect individual will be unco-operative or unwilling to assist in any circumstances other than by compulsion, and assuming that the investigation is into a serious or complex fraud of the type that would fall under the remit of the Serious Fraud Office (SFO), a MLA request can be made to direct the SFO to obtain such evidence from the individual using its compulsory section 2 powers.[41] Answers obtained via this process are not generally admissible as evidence against the interviewee in criminal proceedings,[42] although they will inform the rest of the investigation.

Before granting the request, the requesting authority will be expected to provide an undertaking that any statement, or the contents of any interview, made by an individual pursuant to a compulsory section 2 notice will not be used in evidence against that person in any subsequent prosecution.[43]

17.3.6 Search and seizure

Under section 16 of CICA, an overseas authority can request the search or seizure of property in the United Kingdom. However, a request will not be granted automatically, even in circumstances where a search warrant has been issued in the requesting country.

See Section 17.3.7

In the first instance, the UK authorities may choose to implement the request less invasively, such as by seeking the production of documents. Moreover, even if the UK authorities accede to the request they do not have the power to grant the search warrant themselves, but must apply to a UK court.

Under section 17 of CICA, a court in England, Wales or Northern Ireland[44] may only issue a warrant at the request of an overseas authority where they are satisfied that the following three conditions are met: first, that criminal proceedings have been instituted, or a person has been arrested during the course of a criminal investigation, outside the United Kingdom; second, that the offence at issue would constitute an indictable offence in England or Wales (or an arrestable offence in Northern Ireland); and third, that there are reasonable grounds to suspect that the premises in question are occupied or controlled by that person and contain evidence relating to the offence.[45]

An application for a search warrant must be supported by a written document, known as an information, setting out the factual basis on which the warrant is sought. Since search warrant applications are made *ex parte*, the officer making the

41 Section 2 of the Criminal Justice Act 1987 (CJA). The Financial Conduct Authority has a similar power under section 171 of the Financial Services and Markets Act 2000 (FSMA).

42 Answers given in compelled interviews will, however, be admissible against the interviewee in most types of non-criminal proceedings.

43 *Saunders v. The United Kingdom* [1996] ECHR 65, para. 68 in particular.

44 Different conditions apply to warrants issued in Scotland (see section 18 CICA).

45 Section 17(3) CICA.

application must furnish the court with the full facts at their disposal (including those that militate against the granting of a warrant).[46]

Where a warrant is granted under section 17 of CICA, an officer from the executing UK authority may enter the property to seize and retain evidence relating to the offence. All search warrants executed in the United Kingdom must comply with the requirements of PACE and Code B.[47] This includes a requirement to provide the occupier of the premises with a copy of the warrant.

Where evidence is seized under CICA, either the original or a copy will be sent via the UKCA to the court in the territory that requested the seizure.[48] However, further considerations will apply in the event that the material seized is subject to legal professional privilege or constitutes 'special procedure material'.[49]

See Chapter 35 on privilege

In this regard, it is worth noting that an individual may hold privileged material belonging not only to themselves, but also to their current or former employer (such as legal advice given to the company or material generated during the course of an internal investigation).[50] In the event of seizure of such material, the company that has the benefit of the privilege may itself wish to make representations to the authority receiving the material.

Production of documents 17.3.7

See Chapter 11 on production of information to authorities

In cross-border investigations involving financial crime, the most common mechanism to compel individuals to produce information, whether by answering questions in interview or by producing documents, is through the SFO's powers under section 2 of the Criminal Justice Act 1987 (CJA).[51]

The territorial scope of the SFO's powers under section 2 is not defined by the CJA. However, in the recent case of *R (KBR Inc) v. Serious Fraud Office*,[52] it was determined that section 2 powers can, in certain circumstances,[53] have extra-territorial effect (circumventing the requirements of MLA).[54] Accordingly, consideration should be given early in any cross-border investigation to what documents

46 *R (Energy Financing Team) v. Bow Street Magistrates' Court* [2006] 1 WLR 1317.

47 Section 15(6) PACE specifies what a warrant should contain.

48 Section 9 CICA.

49 Special procedure material includes journalistic material, or material acquired or created in the course of any trade, business, profession or other occupation, which is held subject to a duty of confidentiality (section 14 PACE 1984).

50 The recent decision in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2018] EWCA Civ 2006 has broadened the scope of material that might arguably be subject to legal professional privilege.

51 Equivalent powers under Part XI of the Financial Services and Markets Act 2000 in respect of FCA investigations and section 62 of the Serious Organised Crime and Police Act 2005 in respect of National Crime Agency, HMRC and police investigations into 'specified offences'.

52 [2018] EWHC 2012 (Admin).

53 The notice was challenged on jurisdictional grounds. However, the High Court ruled that there was a 'sufficient connection' between KBR Inc and the UK.

54 On 8 April 2019, the UK Supreme Court granted KBR Inc leave to appeal the decision, although the basis of the appeal is not known.

an individual has in his or her possession (whether in hard copy or electronically) and where they are held.

In addition, under section 20 of CICA, a participating country[55] may request a freezing order in relation to evidence (this does not extend to property or money). Requests would be made to the Home Office and must relate to a listed offence.[56] Once evidence has been frozen it must be retained until instructions have been received to transfer that evidence to the requesting state, or to release it.[57]

In the future, the Crime (Overseas Production Orders) Act 2019 (COPOA)[58] will enable an 'appropriate officer'[59] to apply to the Crown Court for an overseas production order[60] requiring a person based in a country outside the United Kingdom that is party to, or participates in, a 'designated international co-operation arrangement' to produce or give access to 'electronic data'[61] regardless of where it is stored. At present, no designated agreements are in place, meaning certain operative parts of COPOA are not yet in force. However, the United Kingdom is in the process of negotiating a designated agreement with the United States pursuant to the US Clarifying Lawful Overseas Use of Data Act 2018.

17.4 Extradition

In cross-border criminal investigations, suspects are often resident outside the jurisdiction conducting the investigation.[62] As such, a critical question will be whether, and how, they may be subjected to extradition.

The answer lies in the legislation of, and arrangements between, the requesting and requested states.

The UK position is governed by the EU Framework Decision[63] and its obligations are implemented through the Extradition Act 2003 (the 2003 Act).

---

55 One of the EU Member States, Iceland, Japan, Switzerland and the United States.

56 Article 3, Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence.

57 Section 24 CICA.

58 COPOA received royal assent on 12 February 2019.

59 The 'appropriate officers' include a constable, an officer of HMRC, a member of the SFO and a person appointed by the Financial Conduct Authority (section 2(1)(a) COPOA).

60 The requirements of which the Crown Court judge must be satisfied before granting an overseas production order are set out in section 4 COPOA.

61 'Electronic data' is broadly defined as 'any data stored electronically', although OPOs cannot require the production of material that is protected by legal professional privilege, or personal confidential records relating, for example, to an individual's physical or mental health (section 3 COPOA).

62 The focus of this chapter is on extradition from the United Kingdom. However, individuals wanted by overseas authorities may be the subject of an Interpol red notice. Red notices can be issued on the basis that the individual is sought for prosecution or to serve a sentence. Once issued, a red notice alerts police and border officials around the world, and therefore affected individuals may encounter difficulties when travelling internationally, even if they are not subject to an investigation or arrest warrant in the jurisdiction they are travelling from or to. For more information see: https://www.interpol.int/INTERPOL-expertise/Notices/Red-Notices.

63 2002/584/JHA.

The 2003 Act is divided into two parts. Part 1 applies to requests made by 'category 1 territories' (EU countries and Gibraltar) through the European arrest warrant (EAW) procedure.[64] Part 2 applies to requests made by 'category 2 territories', namely those other countries with which the United Kingdom has extradition relations.[65]

It is not yet clear what impact the United Kingdom's decision to leave the European Union will have, but it is likely that legislators will be revisiting this sometimes controversial area of law.

Extradition from the UK – category 1 territories: the EAW 17.4.1

The EAW is a fast-track procedure that allows the requesting state to secure the return of a requested person quickly and effectively.

The National Crime Agency certifies the EAW on receipt from the requesting state before liaising with the Crown Prosecution Service (CPS) for advice on the validity and content of the request.

The requesting state must identify the offence of which the requested person is accused and confirm that the EAW is issued with a view to his or her arrest and extradition for the purpose of prosecution or, where the requested person has been convicted, for the purpose of being sentenced or to serve a sentence already passed. The information must include details such as the requested person's identity and particulars of the alleged offence or conviction. Failure to comply with these requirements invalidates the EAW.[66]

Following the certification of the EAW, a warrant for the requested person's arrest is issued. On arrest, the individual will initially be taken to a police station and held there under the provisions of PACE and the accompanying Code C. The individual has various rights, including the right to have someone informed of the arrest, the right to free independent legal advice, and the right to consult privately with a solicitor. A formal custody record will be opened, detailing key aspects of the detention, but the individual will not be interviewed as it is not the role of the police to investigate the offence. However, given the significance of identification to the extradition process, fingerprints, non-intimate samples and photographs may be obtained from the individual in accordance with PACE Code D.[67]

Following the requested person's arrest and initial detention, he or she must be brought before a court[68] 'as soon as practicable' for an initial hearing and fixing of the extradition hearing within the next 21 days.[69] Depending on the day and time of the arrest, this requirement can mean that the individual spends only hours in

64 Extradition Act 2003 (Designation of Part 1 Territories) Order (SI 2003/3333).

65 Extradition Act 2003 (Designation of Part 2 Territories) Order (SI 2003/3334).

66 Section 2, the 2003 Act.

67 Sections 166 to 168, the 2003 Act.

68 In England and Wales, cases are heard at Westminster Magistrates' Court; in Scotland, cases are heard at the Edinburgh Sheriff Court; and in Northern Ireland, cases are heard by designated county courts or resident magistrates.

69 Sections 3 and 4, the 2003 Act.

police detention before being brought before the court although, if arrested at the weekend, it can mean spending up to two nights in police custody.

At the extradition hearing, the judge must be satisfied that the alleged conduct constitutes an extraditable offence[70] and that no bar to extradition applies. If the judge orders extradition, and in the absence of any appeal, the requested person must be extradited within 10 days of the order, or later if agreed with the requesting state.

Either party may appeal the judge's decision to the High Court.[71] Thereafter, an appeal may be made to the Supreme Court if the matter concerns a point of law of general public importance.[72]

17.4.2 Extradition from the UK – category 2 territories

Part 2 of the 2003 Act provides for the extradition to those non-EAW territories with which the United Kingdom has bilateral or multilateral extradition treaties.[73]

Such territories are usually required to provide *prima facie* evidence of the case against the requested person unless they are signatories to the European Convention on Extradition,[74] or the United States, New Zealand, Australia or Canada.

Requests must be certified by the Home Secretary as being valid before being sent to the appropriate judge.[75] The judge then considers whether there are reasonable grounds to issue an arrest warrant,[76] which include that the evidence produced would justify the issue of a warrant for the individual's arrest if it were a domestic case.[77]

Once an arrest warrant has been issued and executed, the requested person must be brought before the magistrates' court as soon as practicable. Unless the requested person consents to extradition, the court will fix a date for the extradition hearing, usually within the next two months, and decide whether to grant bail.

At the extradition hearing, the judge must first consider the sufficiency of the extradition request and supporting documentation. If the documents do not meet the requirements set out in section 78(2) of the 2003 Act, the judge must discharge the person whose extradition is sought (the requested person).[78] Where the judge is satisfied that the requirements have been met, he or she will then go on to consider whether the person before the court is the requested person, the

70 Sections 64 and 65, the 2003 Act.

71 Sections 26 to 29, the 2003 Act.

72 Section 32, the 2003 Act.

73 A list of category 2 territories is provided here: https://www.gov.uk/guidance/extradition-processes-and-review.

74 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/024/signatures?p_auth=4WJ8nibX.

75 Sections 69 and 70, the 2003 Act.

76 Sections 137 and 138, the 2003 Act.

77 Section 71, the 2003 Act.

78 Section 78, the 2003 Act.

offences specified are extraditable and copies of the documents have been served on the person.[79]

In cases where *prima facie* evidence must be provided, the judge must then decide if the evidence supporting the request is 'sufficient to make a case'. This is the same test that applies in domestic UK criminal proceedings in determining whether a criminal prosecution should be allowed to continue.

If the judge is satisfied that all the conditions have been met, and that no bars to extradition exist, the matter is referred to the SSHD for his or her decision whether to extradite. Representations may be made by the requested person to the SSHD for consideration when deciding whether to extradite.

See Section 17.4.4

The judge's decision to refer may be appealed within 14 days of the date of the decision and thereafter appeals may be lodged with the High Court or, if appropriate, the Supreme Court.

Extradition from the UK – other territories 17.4.3

For countries that are neither category 1 nor category 2 territories, section 194 of the 2003 Act allows the SSHD to certify that 'special extradition' arrangements have been made between the United Kingdom and that country for the extradition of a person.

These special arrangements must comply with the 2003 Act's Part 2 procedures, and the procedure is then as for a category 2 territory.

In addition, a territory party to an international convention to which the United Kingdom is also a party may, under section 193 of the 2003 Act, be designated a territory to which Part 2 of the 2003 Act applies.[80]

Bars to extradition 17.4.4

Under the 2003 Act a properly issued extradition request will be honoured, unless one of the bars to extradition applies.

Sections 11 and 79 of the 2003 Act set out specific bars to extradition for Part 1 and Part 2 requests respectively. These include but are not limited to the rule against double jeopardy, extraneous considerations and the passage of time.

In addition to the specific bars, there are a number of general bars as detailed below.

The human rights bar 17.4.4.1

Under sections 21, 21A (Part 1 cases) and 87 (Part 2 cases) the judge must determine 'whether extradition would be compatible with the [requested person's] Convention rights' within the meaning of the Human Rights Act 1998.[81]

79 Ibid.

80 SI 2005 No. 46, the Extradition Act 2003 (Parties to International Conventions) Order 2005: provides that a state will only be designated a category 2 territory in this way in relation to conduct to which the convention applies, e.g., drug trafficking offences in contravention of the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

81 Sections 21(1), 21A(1)(a) (Part 1 cases) and 87(1) (Part 2 cases), the 2003 Act.

A request may be refused where it is shown that there are substantial grounds to believe that the requested person, if extradited, faces a 'real risk of exposure to inhuman or degrading treatment or punishment'[82] contrary to Article 3 of the European Convention on Human Rights (ECHR) (for example, in relation to prison conditions in the requesting state); or that the interference with the private and family lives of the requested person, and members of his or her family, contrary to Article 8 of the ECHR, outweighs the public interest in extradition.[83] Arguments under Article 5 of the ECHR (the right to liberty and security)[84] and Article 6 of the ECHR (right to a fair trial)[85] can also be invoked under the human rights bar.

17.4.4.2 The proportionality bar

This bar applies to EAW cases only.[86] When considering a request, the judge may consider the seriousness of the alleged conduct, the likely penalty to be imposed and whether there are alternatives to extradition.

17.4.4.3 The forum bar

The forum bar provides that extradition may be barred if it would not be in the interests of justice.[87] This will be considered where the nature of the criminal conduct means that the alleged offence could potentially be prosecuted in more than one country, and is particularly relevant to parallel or cross-border investigations. It was introduced into the 2003 Act by the Crime and Courts Act 2013 as a result of concern in particular in the context of extraditions to the United States and has been in force as a bar to extradition since October 2013.

Extradition would not be in the interests of justice if the judge decides that a substantial measure of the criminal activity took place in the United Kingdom and, having regard to 'specified matters', the judge decides extradition should not take place.[88] The specified matters include consideration of where most of the loss or harm occurred or was intended to occur; the interests of any victims; any belief of a prosecutor that the United Kingdom is not the most appropriate jurisdiction in which to prosecute; desirability and practicability of all prosecutions relating to the extradition offence taking place in one jurisdiction; and the requested person's connections with the United Kingdom.

82 *Soering v. United Kingdom* (1989) 11 EHRR 439.

83 *HH v. Deputy Prosecutor of the Italian Republic, Genoa* (2012) 3 WLR 90 – summarised conclusions of Baroness Hale re: case law interpreting Article 8.

84 *Shankaran v. India* (2014) EWHC 957 (Admin).

85 *Vincent Brown aka Vincent Bajinja, et al. v. The Government of Rwanda, The Secretary of State for the Home Department* (2009) EWHC 770 (Admin).

86 Section 21A, the 2003 Act.

87 Sections 19B (Part 1 cases) and 83A (Part 2 cases), the 2003 Act; not in force in Scotland.

88 Section 19B(2), the 2003 Act.

The forum bar was successfully invoked in two recent cases concerning extradition to the United States (*Love* and *Scott*).[89] Attempts to appeal these decisions were unsuccessful in both cases.

Settlement considerations 17.5

The scope for an individual to settle cross-border investigations or proceedings is in practice limited and will realistically arise either in circumstances where the individual can obtain an immunity from prosecution or where his or her co-operation in one jurisdiction (whether or not involving a guilty plea) effectively resolves the investigations in other jurisdictions.

Sections 71 to 75 of the Serious Organised Crime and Police Act 2005 (SOCPA) set out the statutory framework in which an individual may enter into such an agreement with a UK prosecutor.[90]

Under section 71, a designated prosecutor[91] may grant a suspect immunity from prosecution subject to certain conditions. These conditions invariably require a suspect's full co-operation with the prosecuting authority in the United Kingdom (and, in the context of cross-border investigations, with all relevant overseas authorities). The section 71 notice, which is prepared in writing, also specifies the offences for which the individual cannot be prosecuted. If, however, the conditions of the notice are breached, the immunity will ordinarily be revoked.

Whereas section 71 grants immunity from prosecution, section 73 requires an individual to plead guilty to the offence, but enables the court to take into consideration the assistance the individual has provided to the authorities. This will often result in a substantial reduction in sentence.[92] For this reason a section 73 agreement is often referred to as a 'co-operating defendant' agreement and, in practice, in cross-border investigations will require the individual to co-operate not only with the UK authorities (which can extend to giving evidence, if required, in any UK proceedings against other suspects) but also with overseas investigating authorities.

Therefore, when advising an individual in a cross-border investigation about the possibility of either form of SOCPA agreement, it will be necessary simultaneously to engage with the other investigating authorities so that, for example, a resolution in the United Kingdom through a section 73 agreement will be reflected by equivalent action by the other investigating authorities (such as a non-prosecution agreement in the United States).

Note also that during parallel and cross-border investigations and proceedings a corporate entity will sometimes commence settlement discussions with the authorities (be they regulators or criminal enforcement agencies).

89 *Love v. Government of the United States and another* [2018] EWHC 172 (Admin) and *Scott v. Government of the United States of America* [2018] EWHC 2021 (Admin).

90 In this context, the UK refers to England, Wales and Northern Ireland.

91 Defined by section 71(4) of SOCPA as a prosecutor from the CPS, HMRC, SFO or the DPP of Northern Ireland.

92 *R v. Dougall* [2010] EWCA Crim 1048.

Within the United Kingdom, such discussions are most likely to be with the SFO or the FCA, or both, and, as regards criminal investigations, they are most likely to be centred on the possibility of the authorities agreeing to a deferred prosecution agreement (DPA).[93]

A DPA can only be concluded between the authority (usually the SFO) and the suspect corporate entity; there is no provision for an individual to enter into a DPA. The use to which the authority can put the information it obtains during the DPA negotiations in criminal proceedings against others, including individuals employed by the corporate entity, is unrestricted.[94] This means that an employee suspect is at great risk of having his or her position seriously compromised, including a heightened risk of criminal prosecution, as a result of the co-operation the employer must demonstrate as a prerequisite to being invited by the authority to enter into DPA negotiations.

If a corporate with which the client is connected enters into a DPA, the client may be named in the statement of facts. The current state of the law is unsatisfactory in that a third party does not have to be notified that he or she may be so named. Further, the terms of a DPA and the supporting statement of facts cannot be altered or modified once approved by the court.[95]

If there are extant criminal proceedings against individuals, or the possibility of such proceedings, protection will be put in place to seek to avoid the risk of the DPA causing prejudice to the individuals facing those proceedings. This will be either by anonymising the name of the entity entering into the DPA and the individuals referred to in the statement of facts[96] or by imposing reporting restrictions on the publication of the statement of facts until the conclusion of the associated proceedings.

In all likelihood, the corporate entity will enter (and conclude) settlement negotiations with the authorities without the knowledge of the individuals involved, let alone their input. In trying to put itself into a position where it can reach a DPA, the corporate entity will be anxious to demonstrate its co-operation with the authority, an obligation under the joint SFO and CPS Code of Practice,[97] and that it has severed its links with those individuals responsible for the misconduct. To allow those individuals to participate in the negotiations, or to be seen to be seeking to protect their position, would be likely to prejudice the position of the corporate entity in the eyes of the authority.

93 Schedule 17, Crime and Courts Act 2013.

94 Paragraph 13(6), Schedule 17, Crime and Courts Act 2013.

95 *SFO v. Tesco Stores Limited* [2019] EW Misc 1 (Crown C), para. 4.

96 For example the DPA in *SFO v. XYZ Limited* (U20150856).

97 Paragraph 2.8.2(i), DPA Code of Practice, Crime and Courts Act 2013.

Reputational considerations 17.6

Throughout any parallel or cross-border investigation or proceeding, those representing an individual must always consider the potential impact on their client's reputation. Reputation may include the client's professional reputation among his or her peers or wider public reputation, particularly if the client is a well-known figure. Matters are further complicated because the individual may have a low profile in one jurisdiction, but a high profile in another, or, despite having a low media profile, may have become embroiled in a high-profile investigation.

An associated issue that can often arise in practice is when the details surrounding the criminal investigation or proceedings are in the public domain and the individual is included in a due diligence database, such as World Check or World Compliance. Entry in these databases, which are largely based on open source (and sometimes unreliable) material, can have a profound effect on an individual's ability to access financial services.

As regards criminal investigations, the case of *Richard v. The BBC* affirmed that, as a starting point, a suspect should not be named by the press.[98] Although this position had already, in effect, been adopted following the Leveson Inquiry in 2012 and the College of Policing's Guidance on the Relationships with the Media in 2013, it was the first time that the UK courts had ruled on the issue.[99]

Although this is undoubtedly a positive step for suspect anonymity in the United Kingdom, there is an obvious caveat in the context of cross-border investigations; namely, that since different jurisdictions have different rules on publishing a suspect's identity, an individual who avoids having their details published by the UK press may nevertheless find themselves named overseas. Furthermore, different considerations will apply where, for example, an individual is charged in a criminal investigation or, in the context of FCA proceedings, 'identified' in corporate decision notices.[100]

Recently in the United Kingdom, reputation management has been seen as a distinct professional discipline, with a number of lawyers specialising in the field. They often work together with, rather than in competition with, those from the more traditional public relations firms and consultancies. In any event, those acting for individuals who have reputational considerations, but who lack their own specialised in-house resource, are best advised to turn to one or more of these specialists at as early a stage as possible and integrate them into the client's team of professional advisers. Only through mutual work as part of an integrated team can properly informed consideration be given on the key issues of whether the client's reputation is at risk and, if so, how it can be best protected without adversely affecting his or her position in the ongoing investigation or proceedings.

98 *Richard v. The British Broadcasting Corporation (BBC) & Anor* [2018] EWHC 1837 (Ch), paras. 248-251.

99 Ibid., para. 234.

100 *Financial Conduct Authority v. Macris* [2017] UKSC 19.

18

Individuals in Cross-Border Investigations or Proceedings: The US Perspective

Amanda Raad, Michael McGovern, Meghan Gilligan Palermo, Zaneta Wykowska and Sara Berinhout[1]

18.1 Introduction

There has been a consistent trend in the United States in the past decade towards increased prosecution of individuals in white-collar cases, including for financial fraud and foreign corruption offences. Following widespread criticism after the 2008 financial crises for failing to criminally charge individual wrongdoers, the US Department of Justice (DOJ) implemented a policy shift towards individual accountability, focusing on prosecuting individuals responsible for corporate misconduct and financial fraud.[2]

Three years into the Trump administration, the DOJ and the Securities and Exchange Commission (SEC) continue to focus on prosecuting and charging individuals in white-collar cases.[3] The number of individuals prosecuted by the

1 Amanda Raad and Michael McGovern are partners, and Meghan Gilligan Palermo, Zaneta Wykowska and Sara Berinhout are associates, at Ropes & Gray LLP.

2 Beginning with the 'Yates Memo', issued in late 2015 by former US Deputy Attorney General Sally Yates, the DOJ instituted a policy emphasising the need for US prosecutors to pursue prosecutions of individuals involved in corporate wrongdoing. To effectuate this policy, the Yates Memo mandated that, for a company to receive any co-operation credit, it must provide the DOJ with 'all relevant facts about the individuals involved in corporate misconduct' in both criminal and civil cases, regardless of the level of their involvement in the alleged misconduct. See Memorandum from Sally Quillian Yates, Deputy Att'y Gen., U.S. Dep't of Justice, Individual Accountability for Corporate Wrongdoing (9 September 2015), https://www.justice.gov/dag/file/769036/download.

3 In recent years, the DOJ has relaxed the rigid requirements of the Yates Memo, no longer requiring companies to identify every person with a role in wrongdoing, regardless of culpability level. However, DOJ policy still mandates that companies identify all individuals who were 'substantially involved in or responsible for the misconduct at issue' to receive any co-operation credit. In the civil context, the DOJ has implemented a 'sliding scale' approach where co-operation credit is

DOJ Criminal Division's Fraud Section substantially increased in 2018 over the preceding years, with 406 individuals charged.[4] And as with the ever-increasing globalisation of the world economy, white-collar enforcement against individuals is increasingly cross-border.[5]

For American white-collar practitioners, this means representing clients in all corners of the world as they navigate cross-border criminal prosecutions, civil enforcement actions and corporate internal investigations. Although there are important distinctions unique to each, many of the issues discussed in this chapter are common to all three. Counsel representing overseas clients will need to consider a host of additional issues, including jurisdiction, extradition and collateral consequences, to name a few.

Preliminary considerations 18.2

Arrest and bail 18.2.1

The first critical issue counsel face in criminal proceedings is counselling a client through arrest and bail. US authorities have various means for apprehending criminal defendants,[6] including arrest in the United States, arrest in a foreign jurisdiction and extradition to the United States, or using Interpol red notices to detain foreign individuals travelling abroad.[7] If a client is arrested abroad, counsel should immediately arrange for experienced local counsel. The availability of provisional arrest and bail pending extradition will depend on the laws of the arresting jurisdiction.

---

awarded based on the degree of co-operation. See Rod J Rosenstein, Deputy Attorney General, U.S. Dep't of Justice, Prepared Remarks for the 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

4 See U.S. Dep't of Justice, Criminal Division Fraud Section Year in Review 2018, https://www.justice.gov/criminal-fraud/file/1123566/download; U.S. Dep't of Justice, Criminal Division Fraud Section Year in Review 2017, https://www.justice.gov/criminal-fraud/file/1026996/download (301 individuals charged in white-collar cases in 2017 and 300 in 2016).

5 For example, one of the DOJ's headline cases in 2018 saw numerous individuals charged in a scheme to pay bribes to government officials in Venezuela in exchange for business with Venezuela's state-owned energy company, Petróleos de Venezuela S.A. (PDVSA), Press Release, U.S. Dep't of Justice, Five Former Venezuelan Government Officials Charged in Money Laundering Scheme Involving Foreign Bribery (12 February 2018), https://www.justice.gov/opa/pr/five-former-venezuelan-government-officials-charged-money-laundering-scheme-involving-forei-0.

6 See U.S. Dep't of Justice, Justice Manual § 9-15.635 (2018), https://www.justice.gov/jm/jm-9-15000-international-extradition-and-related-matters (Justice Manual); see also U.S. Dep't of Justice, Justice Manual: Criminal Resource Manual § 611 (2018), https://www.justice.gov/jm/criminal-resource-manual-601-699 (Criminal Resource Manual).

7 For this reason, counsel engaged during the investigatory phase of a cross-border DOJ investigation should carefully consider the client's exposure to prosecution and risk of arrest while overseas. The client should be advised to carry counsel's contact details at all times. In some cases, and taking into consideration the client's home country, counsel may advise the client to refrain from international travel while the DOJ's investigation is pending.

Arrest in the United States presents its own difficulties. Counsel will need to arrange for the client to appear in US court and apply for bail.[8] In most cases, an overseas client will naturally wish to return home pending proceedings in the United States. However, the client's foreign status may be the very thing that makes it difficult to obtain a bail package allowing international travel. The court is more likely to find that the client poses a flight risk (i.e., a risk of fleeing the jurisdiction to avoid criminal prosecution) due to limited US ties. This concern is greater where the client has substantial financial resources or ties to a country that has not entered into an extradition treaty with the United States.[9] Counsel should discuss these risks with the client and obtain a complete understanding of his or her financial and personal circumstances to submit a bail application that mitigates flight-risk concerns. Even if pretrial release is granted, courts commonly impose a stringent set of conditions to guarantee the defendant's ongoing appearance. These conditions may include, for example, home confinement, restrictions of travel to certain countries or districts within the United States, confiscation of travel documents and electronic monitoring.

18.2.2 Preservation of evidence and maintaining confidentiality

Counsel must promptly ascertain whether the client has physical evidence relating to the matter in question. This may include emails, hard drives, text and instant messaging, financial records, and documentary evidence. Counsel should advise clients of the obligation to preserve and not destroy evidence, and consider whether to procatively collect and review such data.

Counsel will likewise need to preserve the integrity of the client's factual recollection. This includes assessing whether the client has discussed relevant matters with potential co-defendants or other parties. Clients should be advised not to communicate with any third parties regarding the matters under investigation and, in most cases, to cease communications with co-defendants entirely.[10]

18.2.3 Initial conversations with the client

Counsel should meet with the client to assess the facts and available evidence as quickly as possible. These early conversations will inform counsel's strategy for reviewing evidence, pursuing additional lines of inquiry, assessing strategic

8 Under the Bail Reform Act, 18 U.S.C. § 3142(b) & (c)(1)(B), US courts must order a defendant's pretrial release unless the court 'determines that such release will not reasonably assure the appearance of the person as required or will endanger the safety of any other person or the community.' Where a defendant is released, the court must do so 'subject to the least restrictive further condition, or combination of conditions that . . . will reasonably assure the appearance of the person.' On the other hand, a court must order detention if it 'finds that no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of any other person and the community.' Id. § 3142(e).

9 See, e.g., *United States v. Zarrab*, 15-CR-867, 2016 WL 3681423, at *7 (S.D.N.Y. 16 July 2016); *United States v. Epstein*, 155 F. Supp. 2d 323, 326 (E.D. Pa. 2001).

10 Communications with such parties should be through counsel and only pursuant to common interest privilege.

options, identifying potential common interest discussions[11] and determining what resources are needed,[12] such as specialised counsel.[13]

Extradition 18.3

It is of increasing importance that counsel representing individuals in cross-border proceedings have, at a minimum, working knowledge of extradition law given the frequency with which extradition issues arise. In 2019, the United States continued the trend of recent decades of aggressively pursuing extradition, including in white-collar cross-border proceedings involving Foreign Corrupt Practices Act (FCPA), money laundering, and securities and commodities law violations.[14]

Applicable law 18.3.1

The US government often is able to secure the presence of a criminal defendant for trial only with the assistance of foreign authorities. While there are technically no limitations on US authorities' ability to seek extradition of individuals abroad, the United States typically does so through extradition requests made pursuant to a treaty.

Extradition treaties form the basis for extradition law and procedure. Signatory states agree to extradite individuals within their jurisdiction who have been charged with an extraditable offence to the requesting state for trial and punishment.[15] Each treaty specifically defines which offences are 'extraditable'.[16] Most modern treaties permit extradition where the alleged conduct is criminal and

11 See id.

12 Initial discussions with the client should include a detailed and candid conversation about the client's financial resources, goals for how those resources are deployed and the availability, if any, of insurance coverage. Litigating criminal actions has grown increasingly expensive in recent decades. Counsel should ensure that the client has a complete understanding of the resources necessary to defend the case, particularly if the client fights the charges and all the more so if the client is self-funding the representation. Where a client is able to be covered under a 'D&O' (directors and officers) policy or similar liability insurance, counsel may advise the client to retain specialised insurance counsel to assist in obtaining and understanding potential limitations on coverage, for example, policy provisions allowing the insurer to claw back legal fees if the client later pleads or is found guilty of criminal charges.

13 In all cases, it is important to consider at the outset the need for other counsel, including employment counsel, extradition counsel, regulatory counsel or counsel specialising in the privacy laws of the relevant jurisdiction.

14 Bruce Zagaris, *International White Collar Crime: Cases and Materials* 413 (2d ed. 2015), https://www.cambridge.org/core/books/international-white-collar-crime/extradition-and-alternatives/ A89CB30F7457E4EFCD81B046DB0833A5 ('According to the Department of State, U.S. courts certified 137 extradition requests between 1945 and 1960 – an average of only 9 per year. In 1995, in contrast, the U.S. extradited 79 people to other countries and received custody of 131.').

15 See Ronald J Hedges, Federal Judicial Center International Litigation Guide: International Extradition: A Guide for Judges 1, 4 (2014), https://www.fjc.gov/sites/default/files/2014/International-Extradition-Guide-Hedges-FJC-2014.pdf.

16 For instance, the treaty between Albania and the United States includes an inventory of more than two dozen crimes. Extradition Treaty, Alb.-U.S., art. 2, 1 March 1933, 49 Stat. 3313.

punishable as a felony in the signatory states (the 'dual criminality' approach).[17] Treaties may also specify which offences are not extraditable, for example military offences or those punishable by death.[18] Other common provisions include prohibitions on double jeopardy, limitation periods and restrictions on the extradition of nationals.[19]

To date, co-operation has bilateral extradition treaties with approximately two-thirds (over 100) of the world's nations[20] and is party to two multilateral extradition agreements.[21]

18.3.2 Extradition procedure

Extradition procedure is determined by treaty, the responding state's extradition laws, and considerations of diplomacy and foreign policy. Typically, US authorities must first obtain approval from the DOJ's Office of International Affairs (OIA).[22] The OIA advises prosecutors regarding what filings are required under the applicable treaty, and the US Department of State issues a formal request to

17 Justice Manual, supra note 6, § 9-15.635 (2018); see also Criminal Resource Manual, supra note 6, § 603.

18 See, e.g., Extradition Treaty, U.K.-U.S., art. 4(1)-(2), 31 March 2003, T.I.A.S. 07-426 (UK Extradition Treaty).

19 Historically, the most common extradition treaty provision provided that signatory countries were not required to extradite their own citizens. See M Cherif Bassiouni, International Extradition: United States Law and Practice 746 (6th ed. 2014). This practice has evolved, however, and many modern treaties contain provisions either prohibiting signatory countries from denying extradition on the basis of nationality, or providing that denial on the basis of nationality is permissible only if the case is referred to local authorities for prosecution. See, e.g., U.K. Extradition Treaty, supra note 18, art. 3; Extradition Treaty, Peru-U.S., art. 3, 26 July 2001, T.I.A.S. 03-825; Extradition Treaty, Belize-U.S., art. 3, 30 March 2000, T.I.A.S. 13089; Extradition Treaty, Para.-U.S., art. 3, 9 November 1998, T.I.A.S. 12995; Extradition Treaty, S. Kor.-U.S., art. 3, 9 June 1998, T.I.A.S. 12962; Extradition Treaty, Pol.-U.S., art. 4, 10 July 1996, T.I.A.S. 99-917. Certain countries do, however, continue to prohibit extradition of their nationals but retain the discretion to do so. See, e.g., Extradition Treaty, Fr.-U.S., art. 3(1), 23 April 1996, T.I.A.S. 02-201 (France Extradition Treaty); Extradition Treaty, Ger.-U.S., art. 7(1), 20 June 1978, 32 U.S.T. 1485.

20 See U.S. Dep't of State, Treaties in Force: A List of Treaties and Other International Agreements of the U.S. in Force on January 1, 2019, https://www.state.gov/wp-content/uploads/2019/06/2019-TIF-Bilaterals-6.13.2019-web-version.pdf.

21 See Inter-American Convention on Extradition, 26 December 1933, 49 Stat. 3111 https://www.oas.org/juridico/MLA/en/Treaties/en_Conve_Extra_Inter_American_1933_Montevideo.pdf; Extradition Agreement, European Union-U.S., 25 June 2003, S. Treaty Doc. No. 109-14, https://www.congress.gov/109/cdoc/tdoc14/CDOC-109tdoc14.pdf. In addition, the United States is party to several multilateral international conventions that further reinforce bilateral extradition treaties by binding member states to either extradite or prosecute individuals charged with particular offences. See, e.g., United Nations Convention for the Suppression of Unlawful Seizure of Aircraft art. 8, 16 December 1970, 860 U.N.T.S. 105; United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances art. 6, 20 December 1988, 1582 U.N.T.S. 95.

22 Justice Manual, supra note 6, § 9-15.210.

the responding state.[23] The responding state's judiciary then determines whether extradition is permissible.[24]

The US government may also seek provisional arrest, namely a request to the responding state to arrest the individual pending submission of a formal extradition request.[25] The DOJ deems provisional arrests appropriate where there is a risk that the individual will flee the foreign jurisdiction.[26] The conditions under which provisional arrest is permissible, and the duration an individual may be held until a formal request is filed,[27] vary by treaty.[28]

The timeline for extradition to the United States varies depending on the circumstances of the case and the responding state involved.[29] On average, it takes more than a year from the time the formal request is made until the individual is surrendered to US authorities.[30] While US courts have held that the Speedy Trial Clause of the Sixth Amendment requires that extradition be sought as soon as the individual's location becomes known,[31] this has no bearing on how long it takes

23 Id. § 9-15.300.

24 Specifically, the presiding judge in the foreign jurisdiction will confirm the identity of the individual, that the relevant treaty and domestic laws support extradition for the alleged offence, that the complaint filed by the United States sets forth sufficient facts to support probable cause to believe that the alleged offence was committed, and that all other elements of the extradition request comply with treaty provisions. See Hedges, supra note 15, at 10-11. The individual is then provided an opportunity to challenge the validity of the extradition request on various factual and procedural grounds. The Federal Rules of Criminal Procedure, Civil Procedure and Evidence do not apply in extradition proceedings. See *In re Requested Extradition of Kirby*, 106 F.3d 855, 867 (9th Cir. 1996) (Noonan, J., dissenting); Fed. R. Evid. 1101(d)(3); Fed. R. Crim. P. 1(a)(5). Accordingly, hearsay evidence and unsworn statements may be admissible. See, e.g., *Haxhiaj v. Hackman*, 528 F.3d 282, 292 (4th Cir. 2008); *Zanazanian v. United States*, 729 F.2d 624, 626 (9th Cir. 1984); *Collins v. Loisel (Collins II)*, 259 U.S. 309, 317 (1922); *Artukovic v.* Rison, 784 F.2d 1354, 1356 (9th Cir. 1986).

25 All modern US extradition treaties include articles providing for provisional arrest. See S. Exec. Rep. No. 106-26, at 31 (2000) (report from U.S. Senate Committee on Foreign Relations); see, e.g., Extradition Treaty, Canada-U.S., art. 11(1), 3 December 1971, 27 U.S.T. 983.

26 Criminal Resource Manual, supra note 6, § 615.

27 Typically, once a provisional arrest is made, prosecutors have between one and three months to submit a formal extradition request. See Justice Manual, supra note 6, §§ 9-15.210, 9-15.230; see, e.g., Extradition Treaty, Canada-U.S., art. 11(1), 3 December 1971, 27 U.S.T. 983 (requiring release 'upon the expiration of forty-five days from the date of his arrest' if an extradition request is not received within that time).

28 If a client is taken into custody under a provisional arrest warrant, counsel likely will need to advise the client regarding bail, which may be sought in the responding jurisdiction while extradition is pending. Clients may need to mobilise significant resources and assemble bond guarantors to effectuate bail as quickly as possible. For this reason, too, it is essential that experienced extradition counsel in the relevant jurisdiction be engaged to navigate bail issues in the responding state.

29 Justice Manual, supra note 6, § 9-15.400.

30 Jonathan Masters, What is Extradition?, Counsel on Foreign Relations (11 April 2019), https://www.cfr.org/backgrounder/what-extradition.

31 *United States v. Blanco*, 861 F.2d 773, 780 (2d Cir. 1988), cert. denied, 489 U.S. 1019 (1989); *United States v. Pomeroy*, 822 F.2d 718, 720 nn.3-4 (8th Cir. 1987); *United States v. Walton*, 814 F.2d 376, 380 (7th Cir. 1987); see also Criminal Resource Manual, supra note 6, § 601-99.

the responding state to surrender the individual according to its laws or due to other considerations.[32]

18.3.3 Strategic options: litigating or waiving extradition

Key factors affecting the decision to litigate or waive extradition include:

- *Strength of available extradition defences*: The advisability of litigating extradition turns primarily on whether it can be resisted successfully. While there are several defences available to extradition, they are limited.
- *Strength of evidence in the US criminal case*: The strength of US authorities' evidence of the charged crimes is also relevant. If the evidence is strong and there may be viable extradition defences, attempting to defeat extradition may be the best (and perhaps only) way to avoid liability on the criminal charges.[33] If, however, the evidence is strong and there are no viable or weak extradition defences, it is advisable to consider how best to mitigate eventual liability in the United States, including by considering consent to extradition in the hope of obtaining a favourable plea offer and sentence.[34] On the other hand, if the

32 For example, extradition proceedings in the foreign jurisdiction may be susceptible to political considerations, which may influence the timeline for extradition and even whether it occurs at all. The US government's ongoing effort to extradite WikiLeaks founder Julian Assange from the United Kingdom is a prime example. After a long criminal investigation beginning in 2010, Mr Assange was charged by US authorities in 2018 with conspiracy and espionage related to the leak of classified documents. See Indictment at 4-6, *United States v. Assange*, No. 1:18-cr-111 (E.D. Va. 6 March 2018), https://www.justice.gov/opa/press-release/file/1153486/download. After spending seven years in the Ecuadorian embassy in London resisting extradition in connection with an unrelated prosecution in Sweden, Mr Assange lost the extradition case and Ecuador withdrew his asylum in early 2019. See *Assange v. Swedish Prosecution Auth.* [2011] EWHC 2849. He was thereafter arrested by UK authorities on a provisional arrest warrant in 2019 and faces an extradition hearing in the United Kingdom in 2020. Current political uncertainties, likely will impact whether Mr Assange is ultimately extradited to the United States. See John T Nelson, L'Affaire d'Assange: Why His Extradition May Be Blocked, Just Security (7 June 2019), https://www.justsecurity.org/64425/laffaire-dassange-why-his-extradition-may-be-blocked/.

33 This approach, however, requires careful consideration of the collateral consequences of successfully defeating extradition, including the possibility that the United States may bring new charges and initiate another extradition proceeding even after their first attempt at extradition fails. In addition, the client likely will be effectively prohibited from travelling to any country with which the United States has an extradition agreement because of the risk that the United States could initiate extradition proceedings in that jurisdiction.

34 Another consideration relevant to assessing the strength of the evidence is that a client is not legally entitled to discovery from the US government related to the underlying criminal charges until he or she makes an appearance in a US court. While the foreign court presiding over the extradition proceeding may have have discretion to grant discovery pursuant to its 'inherent power', any discovery obtained (if at all) will be limited in scope and nature. See *Quinn v. Robinson*, 783 F.2d 776, 817 n.41 (9th Cir. 1986); see also *Oen Yin-Choy v. Robinson*, 858 F.2d 1400, 1407 (9th Cir. 1988). Accordingly, in most cases, clients will not receive any discovery until extradited (by force or consent), making it challenging to accurately assess the strength of the government's evidence. Counsel likely will have access only to evidence the client has in his or her possession, information gleaned from co-defendants (pursuant to a joint defence agreement), and evidence provided by the US government, which is likely to be scant (or non-existent) if the client is resisting extradition.

client has a strong case to defend against the underlying charges, he or she may wish to waive extradition, fight the charges in the United States, and attempt to assert the rule of speciality should the United States later try to supersede with additional or more serious charges.[35]

- *The client's goals*: Clients may nonetheless prefer to defer extradition for personal, family or similar reasons, even if they are unlikely to succeed. For example, if the client has health issues requiring treatment, or wants to remain close to relatives, it may be prudent to litigate. Conditions of confinement may also impact the decision, for example, if the client obtains a favourable bail package in the arresting state, he or she may prefer to delay extradition to the United States, where bail conditions may be uncertain and conditions of confinement more difficult.
- *Costs and resources*: Litigating extradition is expensive and resource-intensive. Clients, especially those with limited resources, may wish to direct finite resources to fighting the underlying criminal case.

These considerations must be balanced against the risk that if the United States successfully extradites the client, authorities likely will view prior resistance to extradition as avoiding responsibility or purposefully delaying the criminal case. Both could negatively impact the disposition of the case, impeding an effort to secure bail upon extradition and foreclosing or limiting favourable plea offers, co-operation opportunities, or sentencing recommendations.[36]

If a client waives extradition, the procedure typically involves filing an affidavit of consent in the responding state acknowledging that the extradition requirements have been met.[37] Individual states may have additional requirements to perfect waiver. Not all treaties allow waiver, in which case waiver may be denied.[38]

Regardless of which option a client chooses, it is critical to retain extradition counsel in the responding state. Extradition proceedings have serious implications

35 US courts are divided on whether an individual defendant has standing to raise a 'rule of specialty' challenge. In some circuits, the defendant has the right to raise a doctrine of specialty challenge. See, e.g., *United States v. Stokes*, 726 F.3d 880, 889 (7th Cir. 2013) (collecting cases). Other circuit courts hold, on the other hand, that rule of specialty objections can be raised only by the sending nation, not the individual defendant. See, e.g., *United States v. Suarez*, 791 F.3d 363, 366-67 (2d Cir. 2015); *United States ex rel. Saroop v. Garcia*, 109 F.3d 165, 168 (3d Cir. 1997). Some of the remaining circuits take the middle ground, allowing the defendant to raise a rule of specialty claim unless the sending nation consents to the deviation, while others still have not expressed an opinion. See *Stokes*, 726 F.3d at 889 (collecting cases). See note 40 infra.

36 This risk is particularly acute for clients who are likely to become co-operating witnesses or plead guilty, as US authorities typically view resisting extradition as non-co-operation. For this reason, it is not uncommon for US authorities to require waiver of extradition as a precondition to co-operation or before they will even consider the client as a potential co-operating witness.

37 Hedges, supra note 15, at 8-10.

38 See Bruce Zagaris, U.S. Efforts to Extradite Persons for Tax Offenses, 25 Loy. L.A. Int'l & Comp. L. Rev. 653, 676 (2003) (US extradition treaties that entered into force prior to 1980 do not provide for waiver of extradition); see, e.g., Extradition Treaty, Austl.-U.S., 8 May 1976, 27 U.S.T. 957; France Extradition Treaty, supra note 19, art. 3(1).

for a client's liberty and involve multiple foreign jurisdictions. Experienced counsel is necessary to identify potential defences, attend court appearances, and communicate with foreign counterparts.

18.3.4 Defences to extradition

Defences to extradition are limited, as the responding state generally must grant extradition provided treaty requirements are met. Ultimately, the specific language of the treaty at issue and, in some cases, the laws of the responding jurisdiction,[39] determine which defences are available.[40] Common defences include:

See Chapter 17 on individuals in cross-border proceedings: the UK perspective

- *Where the offence occurred*: Historically, many treaties did not permit extradition for crimes for which the United States asserts extraterritorial jurisdiction.[41] Another example of the location of the alleged misconduct operating as a defence is found in the UK's 'forum bar', which has recently been successfully invoked in multiple cases. The majority of modern treaties now require extradition regardless of where the offence occurred or allow extradition provided that the signatory countries' criminal laws are compatible.[42]
- *Nature of the offence*: The next defence is whether the offences in question are extraditable under the language of the applicable treaty. For example, in dual criminality treaties, extradition typically is denied where the alleged offence is not a crime in the responding state.[43]

39 For instance, in the United Kingdom, local law provides several specified grounds for defending against extradition. See Extradition Act 2003, c. 41, §§ 81, 87, 13.

40 Defences that may be available to a client upon arriving in the United States for trial typically are not available at the extradition stage. For example, the foreign judge presiding over the extradition proceeding may refuse to admit evidence supporting a defence of insanity or alibi, which may be raised as defences to the underlying substantive offences in the US criminal proceeding. See, e.g., *Charlton v. Kelly*, 229 U.S. 447, 462 (1913) (holding that the extradition magistrate properly excluded the evidence of insanity at the hearing stage); see also *Shapiro v. Ferrandina*, 478 F.2d 894, 901 (2d Cir. 1973). These defences are likely to be available only when the client arrives in the United States. Similarly, once a client has been extradited to the United States, he or she may assert the rule of specialty, which provides that defendants may be tried by the requesting state only for the specific offences for which extradition is granted. See *United States v. Lopesierra-Gutierrez*, 708 F.3d 193, 205–06 (D.C. Cir. 2013); *United States v. Lomeli*, 596 F.3d 496, 501 (8th Cir. 2010).

41 Criminal Resource Manual, supra note 6, § 603.

42 See, e.g., Extradition Treaty, Jordan-U.S., art. 2(4), 28 March 1995, S. Treaty Doc. No. 104-3; Extradition Treaty, Austria-U.S., art. 2(6), 8 January 1998, T.I.A.S. 12916; Extradition Treaty, Lux.-U.S., art. 2(1), 1 October 1996, T.I.A.S. 12804; Extradition Treaty, Hung.-U.S., art. 2(4), 1 December 1994, T.I.A.S. 97-318; Extradition Treaty, Bah.-U.S., art. 2(4), 9 March 1990, T.I.A.S. 94-922; France Extradition Treaty, supra note 19, art. 2(4).

43 See, e.g., UK Extradition Treaty, supra note 18, art. 2(1). This defence may be particularly relevant in the FCPA context, as many countries do not outlaw certain forms of payment to government officials that are prohibited as bribery under the FCPA. For example, in 2005, the US authorities indicted a Czech national residing in The Bahamas for participating in a scheme to bribe foreign government officials. Despite the existence of a U.S.-Bahamian extradition treaty, the Bahamian courts ruled that the defendant could not be extradited because the charges against him were for

- *Procedural issues*: Procedural defences may be available based on deficiencies in the extradition proceeding,[44] for example insufficiencies in the United States' filings such as a lack of signature or failure to produce the warrant.[45] Counsel also should consider whether any statute of limitations or double jeopardy defences apply.[46]
- *Humanitarian considerations*: Humanitarian defences may apply. Many states deny extradition where the requesting state may pursue the death penalty[47] or has inhumane prison conditions.[48] A handful of states allow individuals to assert lack of mental competency as a defence.[49] However, humanitarian defences often can be defeated by the US government by certain undertakings, for example agreement that the United States will not seek the death penalty.[50]

Appealing extradition orders 18.3.5

Although extradition orders typically are not appealable,[51] counsel should consult with experienced counsel in the responding state, as local law may allow for appeal.[52] Even if no appeal is made, the United States may file a new complaint

---

acts that, if committed in the Bahamas, would not constitute a crime. See *Superintendent of Her Majesty's Foxhill Prison & U.S. v. Kozeny,* Privy Council Appeal No. 0073, § 53 (Judicial Comm. of the Privy Council 28 March 2012) (Bah.).

44 Justice Manual, supra note 6, §§ 9-15.240, 9-15.250.

45 Id. § 9-15.240.

46 These defences typically can be raised only where the applicable treaty specifically provides for such defences. See *In re Extradition of Chan Seong-I*, 346 F. Supp. 2d 1149, 1157 (D.N.M. 2004); *United States v. Neely*, 429 F. Supp. 1215, 1225 n.9 (D. Conn. 1977); Michael John Garcia & Charles Doyle, Cong. Research Serv., 98-958, Extradition to and from the United States: Overview of the Law and Recent Treaties 15–16 (2010), https://fas.org/sgp/crs/misc/98-958.pdf (citing extradition treaties that include provisions addressing lapse of time); UK Extradition Treaty, supra note 18, arts. 2, 5, 6; *In re Ryan*, 360 F. Supp. 270, 275 (E.D.N.Y. 1973), aff'd, 478 F.2d 1397 (2d Cir. 1973).

47 See, e.g., UK Extradition Treaty, supra note 18, art. 7.

48 For instance, in May 2019, a Dutch court suspended the extradition of an individual to the United Kingdom due to 'inhuman or degrading' conditions in a British prison. See Kaya Burgess & Jonathan Ames, Dutch court refuses extradition to UK's 'inhumane' prisons, *The Times* (11 May 2019), https://www.thetimes.co.uk/article/dutch-court-refuses-extradition-to-uk-s-inhumane-prisons-w9dvjkqpm.

49 Jennifer Piel et al., Determining a Criminal Defendant's Competency to Proceed With an Extradition Hearing, 43 J. Am. Acad. Psychiatry & L. 201, 202-03 (June 2015), http://jaapl.org/content/jaapl/43/2/201.full.pdf.

50 In 2001, for example, the Supreme Court of Canada ruled that it would not extradite two individuals who allegedly confessed to a brutal triple murder unless the Canadian government received assurances that the individuals would not be subject to the death penalty in the United States. Canada is entitled to seek such assurances under its extradition treaty. Extradition Treaty, Canada-U.S., art. 6, March 22, 1976, 27 U.S.T. 983.

51 *Collins v. Miller*, 252 U.S. 364, 369 (1920) ('proceeding before a committing magistrate in international extradition is not subject to correction by appeal'); *In re Mackin*, 668 F.2d 122, 127-28 (2d Cir. 1981) (citing over a dozen cases holding the same).

52 In the United Kingdom, for example, extradition decisions are appealable by both the individual and requesting state. Extradition: processes and review, Gov.UK, https://www.gov.uk/guidance/extradition-processes-and-review#extradition-from-the-uk-category-2-territories.

to begin a separate extradition proceeding if unsuccessful in the first. Courts have uniformly held that there is no limit to how many times the United States may renew an extradition request,[53] even when based on the same evidentiary facts as the earlier request and regardless of whether it was previously denied on the merits or procedural grounds.[54] Similarly, clients may always challenge an adverse extradition ruling by petitioning for a writ of habeas corpus in the United States.[55] The US court's ruling on such a petition is appealable,[56] and the court may choose to stay the foreign extradition proceeding during the appeal.[57]

18.3.6 Recent developments

2019 saw significant extradition activity. New extradition treaties took effect, including treaties between the United States and Serbia and Kosovo.[58] The US government also sought and successfully executed a number of extraditions.[59] In perhaps the highest-profile case of 2019, UK authorities provisionally arrested

53 See *Collins v. Loisel*, 262 U.S. 426, 429 (1923) (holding that double jeopardy does not apply to extradition decisions).

54 Renewed requests are generally heard by a different judicial officer and reviewed de novo. See *Ahmad*, 910 F.2d 1063, 1065 (2d Cir. 1990); *In re Extradition of Mackin*, 668 F.2d 122, 137 n.20 (2d Cir. 1981); *Hooker v. Klein*, 573 F.2d 1360, 1369 (9th Cir. 1978); *In re Gonzalez*, 217 F. Supp. 717, 720 (S.D.N.Y. 1963). Subsequent extradition requests may be based exclusively on evidence submitted in the initial request or supplemental evidence. See, e.g., *Hooker*, 573 F.2d at 1366 (government's renewal of its extradition request was valid despite its first request being 'denied following an extensive evidentiary hearing and full consideration of the merits of the case by an extradition court'); accord *Mirchandani v. United States*, 836 F.2d 1223, 1226 (9th Cir. 1988); *In re Extradition of Tafoya*, 572 F. Supp. 95, 97 (W.D. Tex. 1983); cf. *Ahmad v. Wigen*, 726 F. Supp. 389, 397 (S.D.N.Y. 1989), aff'd 910 F.2d 1063 (2d Cir. 1990); see also *Ntakirutimana v. Reno*, 184 F.3d 419, 423 (5th Cir. 1999); *In re Extradition of Mackin*, 668 F.2d 122, 137 n.20 (2d Cir. 1981).

55 See 28 U.S.C. § 2241; see, e.g., *Ahmad*, 910 F.2d at 1065 ('An extraditee's sole remedy from an adverse decision is to seek a writ of habeas corpus; the Government's sole remedy is to file a new complaint.'). The scope of habeas review is narrower than traditional appellate review and essentially limited to three inquiries: (1) the adequacy of the trial judge's jurisdiction; (2) whether the offence is covered by the relevant treaty; and (3) whether there was sufficient evidence to support probable cause. John T. Parry, The Lost History of International Extradition Litigation, 43 Va. J. Int'l L. 93, 97 (2002).

56 Criminal Resource Manual, supra note 6, § 622.

57 The writ of habeas corpus may be filed before an individual is extradited to the United States. However, the DOJ takes the view that '[t]he filing of the [habeas] petition does not automatically stay further proceedings, and in certain cases the government may go forward with the extradition if the proceedings are not stayed by the order of the [US federal] court.' Criminal Resource Manual, supra note 6, § 622.

58 U.S. Dep't of State, 2019 Treaties and Agreements, https://www.state.gov/2019-TIAS/.

59 Among others, the United States was successful in extraditing an individual from Kosovo under the new extradition treaty with that state for his alleged involvement in a multimillion-dollar securities fraud. See U.S. Dep't of Justice press release, 'Manhattan U.S. Attorney Announces Extradition of Kosovar Man for Securities Fraud Offenses' (26 August 2019), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-extradition-kosovar-man-securities-fraud-offenses.

WikiLeaks founder Julian Assange to face extradition to the United States.[60] Extradition for FCPA offences also continued to be active,[61] consistent with the DOJ's and SEC's increasingly broad view of their mandate to enforce the FCPA.[62]

Strategic considerations 18.4

There are a number of strategic considerations counsel must bear in mind in advising a white-collar client navigating a criminal, civil or internal investigation or proceeding. While certain of these considerations are common to all three contexts, others are particular to criminal actions or internal investigations.

Assessing the client's status 18.4.1

In all three contexts – criminal, civil and internal – counsel must first assess a client's status with respect to a current or potential criminal action (should one later be initiated). Individuals who come into the orbit of a US criminal investigation fall into one of three categories: witness, subject or target.[63] Counsel must

60 Mr Assange continues to fight the extradition case, which is expected to last years. See supra note 32; Isaac Stanley-Becker & William Booth, Julian Assange, expelled from his embassy perch, will fight extradition from jail, Washington Post (12 April 2019), https://www.washingtonpost.com/world/europe/julian-assange-expelled-from-his-embassy-perch-will-fight-extradition-from-jail/2019/04/12/d388584c-5cb2-11e9-98d4-844088d135f2_story.html. While the particular defences Mr Assange intends to raise are yet unknown, it is likely that he will argue, at a minimum, that the charges against him are political, rather than criminal, and therefore extradition would violate the U.S.-U.K. extradition treaty. Lauren Said-Moorhouse & Muhammad Darwish, Julian Assange starts extradition fight from UK prison, CNN (2 May 2019), https://www.cnn.com/2019/05/02/uk/julian-assange-extradition-fight-gbr-intl/index.html; see U.K. Extradition Treaty, supra note 18, art. 4(1). ('[E]xtradition shall not be granted if the offense for which extradition is requested is a political offense.').

61 For example, in May 2019, a Malaysian national previously arrested in Malaysia waived extradition and made his first appearance in US federal court to face charges for conspiring to engage in a multibillion-dollar money laundering scheme and violate the FCPA by bribing foreign public officials to embezzle billions of dollars from 1MDB, Malaysia's sovereign wealth fund. See U.S. Dep't of Justice press release, 'Former Banker Extradited from Malaysia to United States to Face Charges in Multi-Billion Dollar Money Laundering and Bribery Scheme Relating to the 1MDB Fund' (6 May 2019), https://www.justice.gov/opa/pr/former-banker-extradited-malaysia-united-states-face-charges-multi-billion-dollar-money. Notably, the Malaysian authorities have described the defendant's extradition to the United States. as a 'temporary surrender' so that they might later pursue charges for similar conduct brought against him in Malaysia. See Matthew Goldstein, Former Goldman Sachs Banker Pleads Not Guilty in Malaysia Fraud Case, *N.Y. Times*, 6 May 2019 at B3, https://www.nytimes.com/2019/05/06/business/goldman-sachs-roger-ng-1mdb.html.

62 See generally U.S. Dep't of Justice & U.S. Sec. Exch. Comm'n, A Resource Guide to the U.S. Foreign Corrupt Practices Act 11 (14 November 2012); see also Should FCPA 'Territorial' Jurisdiction Reach Extraterritorial Proportions?, Am. Bar Ass'n, (8 November 2018), https://www.americanbar.org/groups/international_law/publications/international_law_news/2013/winter/should_fcpa_territorial_jurisdiction_reach_extraterritorial_proportions/.

63 Under federal law, a 'witness' is someone who authorities believe has information about facts relevant to a criminal investigation and that assist prosecutors in obtaining indictments against other individual or companies. A 'subject,' by contrast, is a 'a person whose conduct is within the

assess the client's status to advise on strategic options, which will vary depending on status. For this reason, it is common for counsel to seek clarification from the DOJ regarding a client's status. However, even if a client is a witness, the designation may change as the investigation progresses. It is therefore critical to independently and continuously assess the client's exposure to advise on the relevant risks and strategic options.

18.4.2 Decision to co-operate

18.4.2.1 Co-operating with or defending a criminal or civil proceeding

A client facing criminal or civil prosecution must choose whether to co-operate with authorities or fight the case.[64] Co-operation may be an attractive option to reduce the potential sentence or financial penalties. But these potential benefits are not without risks. The client must understand the duties that accompany co-operation, including admitting criminal conduct, meeting with the government to provide information about his or her (and others') involvement, and potentially testifying against others at trial. The client also must disclose any other potential misconduct, even if outside the scope of the investigation, and be fully transparent about his or her finances. In determining whether to recommend co-operation, counsel should assess the quality of the client's information, its likely usefulness to the government's case, and the client's capacity for candour and ability to endure probing proffer sessions or trial.

Co-operation typically begins with attorney proffers, during which counsel 'previews' for the government the information that the client can provide.[65] The client will then typically meet with the government for multiple proffer sessions before entering into a formal co-operation agreement to resolve the charges. Client proffers should typically be conducted only after negotiating a proffer agreement, which provides limited protections from the government's future use

scope of the grand jury's investigation,' i.e., someone who engaged in activity or conduct at issue in the prosecutor's investigation, but who the prosecutor has not yet determined participated in criminal activity. A 'target' is 'a person as to whom the prosecutor or the grand jury has substantial evidence linking him to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant.' Justice Manual, supra note 6, § 9-11.151.

64 The government often relies on co-operating witnesses in white-collar cases, both during the investigatory phase and also at trial, e.g., to explain otherwise complicated and document heavy cases. See, e.g., *Kastigar v. United States*, 406 U.S. 441, 446 (1972) ('[M]any offenses are of such a character that the only persons capable of giving useful testimony are those implicated in the crime.') Individual co-operators tend to be lower-level employees or those who are less culpable in the criminal conduct. In particularly complex white-collar cases, the government may rely on more culpable individuals to co-operate against the primary target of an investigation or a company involved in a criminal scheme.

65 During the attorney proffer, counsel should explain to the government counsel's understanding of how the client was involved in the conduct under investigation and outline the information the client will be able to provide to the government. The attorney proffer is a critical opportunity to assess how the government is likely to react to the client's testimony, identify potential risk areas, and potentially learn more about the government's evidence and theory of the case depending upon the prosecutors' questions and reactions.

of any statements made. In addition, before the proffer, counsel should advise the client that he or she cannot be forced to provide information to the government, discuss the consequences of voluntarily speaking with the authorities, and ensure that the client understands the limited protections and potential pitfalls of any proffer agreement.[66]

Clients co-operate with the hope, but no guarantee, of receiving a recommendation from the government for a reduced sentence. Practically speaking, this is delivered in a '5K1.1 letter' from the government recommending a lower sentence than would otherwise be imposed in exchange for co-operation (or 'substantial assistance').[67] Alternatively, clients may receive a deferred prosecution agreement (DPA), under which all charges are dropped after certain conditions are met.[68] A DPA is preferable to a 5K1.1 letter but is harder to obtain.

Many clients choose to co-operate after they have been indicted. In these circumstances, clients usually must decide relatively quickly whether to co-operate, as timeliness of co-operation and acceptance of responsibility will impact the government's plea offer, sentencing recommendation and, ultimately, the court's sentence.[69] Clients may have the opportunity to co-operate pre-indictment, though this typically requires that counsel be involved and proactively engage with the government from the investigation's outset. In these situations, clients may be able

66 The proffer agreement typically includes a provision that the government will not use statements made during the interview directly against the client. See *United States v. Rosemond*, 841 F.3d 95, 109–10 (2d Cir. 2016). However, the government may use the statements for other purposes, e.g., as a lead to obtain other evidence or, if the client later testifies at trial in his own defence, the government can usually offer into evidence contradictory statements made during proffer sessions.

67 Section 5K1.1 of the US Sentencing Guidelines enables the government to make a motion to allow the court to sentence a defendant below the applicable Sentencing Guidelines range. See Federal Sentencing Guidelines Manual § 5K1.1. In such motions, the government typically will set forth the nature, usefulness and significance of the client's assistance during the proffer process. To receive credit for substantial assistance, the client will at a minimum need to be fully transparent about his own illicit conduct and to provide information about other people involved in the criminal activity. The client may also be required to produce documents, participate in investigatory operations (e.g., wearing a wire to record conversations with other defendants or targets), or testify before a grand jury or at trial. Importantly, a 5K1.1 letter is no guarantee of a favourable or reduced sentence, as the court retains discretion to impose a sentence up to the statutory maximum. See Federal Sentencing Guidelines Manual § 5K1.1 (2018) (explaining that a court '*may* depart from the guidelines' in the case of a defendant's substantial assistance to authorities) (emphasis added).

68 A DPA sets out certain conditions that must be met before charges in the indictment will be dropped. Such conditions typically include a fine, term of supervision by pretrial services, or community service. DPAs are typically available only after the client has provided substantial co-operation, including potentially acting as an informant. See, e.g., Enforcement of the FCPA – Criminal Procedures – Deferred Prosecution Agreements, 13 Bus. & Com. Litig. Fed. Cts. § 134:34 (4th ed.).

69 See Federal Sentencing Guidelines Manual § 5K1.1(5).

to resolve the proceedings through a non-prosecution agreement (NPA), in which authorities decline to bring any charges.[70]

Co-operation is not the right path for all clients. Several legal and personal factors may lead the client to fight the case. In those cases, counsel must carefully research and evaluate the client's likelihood of criminal liability and potential defences, including limitation periods and jurisdiction. It is also important to understand the client's personal, financial and family circumstances. Some clients who have a reasonable likelihood of successfully defending the case may nevertheless choose to co-operate because of the collateral consequences of a criminal trial.

18.4.2.2 Co-operating with an internal investigation

In advising a client on co-operating with an internal investigation, counsel should first assess whether the client is a current employee with a duty to co-operate under relevant laws, employment agreements or company policies.[71] If a client is a former employee, he or she nonetheless may be required to co-operate under the terms of any deferred compensation or separation package.[72] Counsel should advise all clients to consider the ramifications of not co-operating on employment prospects and their relationship with the company.

Counsel must also assess whether co-operation will jeopardise Fifth Amendment protections. While private employees generally do not have a Fifth Amendment right against self-incrimination in internal investigations, the right applies where co-operation is compelled (e.g., threat of termination or economic consequence such as unpaid suspension), and the employer's actions are 'fairly attributable' to the government.[73] For example, earlier this year, a federal district court held that an employee's statements were 'compelled testimony' protected by the Fifth Amendment in an internal investigation conducted by his employer at the direction of an enforcement agency.[74] Accordingly, while a client cannot assert the Fifth Amendment in a purely internal investigation, he or she can likely do so where the investigation is conducted at the government's behest, the government

70 To obtain an NPA, the client usually must pay a fine and co-operate with the government. In exchange, the relevant agency will refrain from filing criminal or civil charges. In deciding whether to enter into an NPA, DOJ policy provides that prosecutors should balance the cost of forgoing prosecution with the need for the co-operation to the public interest. Justice Manual, supra note 6, § 9-27.600 (2018).

71 It is now commonplace for employers to write into employment agreements and internal policies a requirement that employees co-operate in internal investigations. Failure to do so can be grounds for disciplinary action, including suspension without pay or termination. It may be necessary to engage employment counsel to advise the client on co-operation obligations under relevant employment agreements, policies or labour law in the relevant jurisdiction.

72 Clients should be made aware that, even where no formal or legally enforceable co-operation obligation exists, employers may withhold deferred compensation or post-employment remuneration to incentivise co-operation with an internal investigation.

73 *Garrity v. New Jersey*, 385 U.S. 493, 497 (1967); see also *United States v. Connolly*, No. 16 CR. 0370 (CM), 2019 WL 2120523, at *10 (S.D.N.Y. 2 May 2019).

74 *Connolly*, 2019 WL 2120523, at *14.

has substantial input into the investigation or the government has effectively 'outsourced' its investigation to the employer or its counsel.[75]

See Chapter 10 on co-operating with authorities and Chapter 14 on employee rights

Finally, counsel must consider the criminal, civil or regulatory consequences of co-operation, including the possibility that the company will share the substance of the client's interview with criminal or civil enforcement authorities.[76] While the client's communications during such interviews are typically privileged in the United States, the underlying facts are not. Further, the privilege belongs to the employer,[77] and the employer may choose to waive privilege, including through self-reporting or compelled disclosure.[78] By the same token, counsel should consider the consequences of not co-operating, particularly in jurisdictions such as the United Kingdom, where FCA-approved persons have an positive obligation to co-operate and failure to do so could jeopardise licensed status.[79]

See Chapter 8 on witness interviews

Dealing with multiple authorities 18.4.3

Voluntary interviews 18.4.3.1

An additional consideration that often arises in cross-border proceedings is how evidence collected and statements made in one jurisdiction can be used by authorities in another. This issue is increasingly important because the United States is more frequently coordinating white-collar investigations with foreign authorities. It has also become common for foreign authorities to conduct parallel investigations into the same or related conduct, regardless of whether there is express coordination with US authorities.[80]

Counsel must consider what impact investigations and corresponding procedures in other jurisdictions may have on US proceedings. One key consideration in this respect is whether a client might waive Fifth Amendment rights by testifying in a foreign proceeding, opening the door for that testimony to be used against the client in a present or future criminal or civil proceeding against the

75 See id. at *11-14. On the other hand, if the company acted entirely on its own, the resulting statements are not 'compelled' by state actors within the meaning of the Fifth Amendment and are therefore freely usable by the government at any later point in time.

76 For example, counsel should carefully assess whether co-operation will increase the risk that a parallel criminal action is brought against the client by US prosecutors or by civil authorities in a foreign jurisdiction in which the client is licensed or regulated.

77 Company counsel likely will inform the client accordingly in an *Upjohn* warning at the beginning of any interview. See *Upjohn*, 449 U.S. 383, 394 (1981); Model Rules of Prof'l Conduct r. 1.13(f), 4.3. Counsel should similarly advise clients, particularly where they may provide information that could be used against them in a future enforcement proceeding.

78 The company may even decide to turn over the notes or summaries of the interview, or may be required to do so under the laws of the relevant jurisdiction.

79 See *Statement of Principle and Code of Practice for Approved Persons*, U.K. Fin. Conduct Auth., § 2.1A.3 (September 2019), https://www.handbook.fca.org.uk/handbook/APER.pdf (Statement of Principle 4 provides that '[a]n *approved person* must deal with the *FCA*, the *PRA* and other regulators in an open and cooperative way and must disclose appropriately any information of which the *FCA* or the *PRA* would reasonably expect notice') (emphasis in original).

80 See, e.g., infra note 81.

client in the United States.[81] Providing some comfort to clients who are compelled to provide testimony in foreign proceedings, at least one US court has held that the Fifth Amendment's prohibition on the use of compelled testimony extends to testimony compelled by a foreign authority, 'even when the testimony was compelled . . . in full accordance with [foreign] law'.[82]

Counsel should also consider whether a client's voluntary interview with a foreign authority would require discussion of subject matter otherwise protected by the attorney–client privilege and therefore waive privilege, permitting US authorities to use that information in their own proceedings. In these situations, it is often advisable to consult with local counsel to confirm the client's obligations and potential risks of refusing the interview request in the foreign jurisdiction.

18.4.3.2 Evidence obtained pursuant to mutual legal assistance treaty (MLAT)

If a client does not co-operate, US authorities may seek testimonial or documentary evidence via an MLAT request.[83] The MLAT process can be slow, taking more than a year between the time a request is made and the time testimony is taken or documents produced.[84] Although most MLATs permit the requesting authority to be present during questioning, the interviews are typically conducted by foreign law enforcement officials pursuant to local procedural rules. This means that certain protections available in the United States may not apply, for example the

81 U.S. Const. amend. V; see *United States v. Saechao*, 418 F.3d 1073 (9th Cir. 2005).

82 *United States v. Allen*, 864 F.3d 63 (2d Cir. 2017) (reversing convictions of two Rabobank traders who provided testimony to the UK's Financial Conduct Authority (FCA) in an investigation into LIBOR manipulation under threat of prosecution for non-cooperation under UK law, because the Fifth Amendment 'prohibits the use and derivative use of such compelled testimony in an American criminal case against the defendant who provided that testimony').

83 The United States has entered into MLATs or similar bilateral agreements with approximately 70 states allowing it to enlist the investigatory authority of those states to procure evidence. See Mark A Rush and Jared A Kephart, Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests (20 January 2017), http://m.klgates.com/lifting-the-veil-on-the-mlat-process-a-guide-to-understanding-and-responding-to-mla-requests-01-20-2017/. In addition, the United States is party to an agreement with the European Union that enhances mutual legal assistance mechanisms with EU Member States. See Mutual Legal Assistance Treaty, European Union-U.S., 16 January 1998, T.I.A.S. 12923. The DOJ's OIA, together with the Department of State, negotiates and implements MLATs, administers mutual legal assistance operations, and coordinates incoming and outgoing requests. Notably, unlike extradition treaties, MLATs generally do not require dual criminality.

84 See United Nations, Manual on Mutual Legal Assistance and Extradition (September 2012), https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf. For this reason, a request for mutual legal assistance to a foreign authority is often accompanied by a petition to a US court under 18 U.S.C. § 3292 to suspend the running of the statute of limitations during the pendency of a request. A court will grant the request if it finds by a preponderance of the evidence that an official request has been made and it reasonably appears that the evidence is or was in a foreign country. See, e.g., T Markus Funk, Federal Judicial Center International Litigation Guide: Mutual Legal Assistance and Letters Rogatory: A Guide for Judges 15 (2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf.

right to counsel or attorney–client privilege. Accordingly, local counsel is essential to navigating the interview process in the foreign jurisdiction.

Counsel selection 18.4.4

A client must also select counsel, which entails deciding whether to engage independent counsel or pursue joint or pool counsel representation with counsel for an employer or colleagues, or both.

Where the representation relates to a client's current or former employment, many employers encourage retaining company counsel, particularly when the client is a current employee. For purely internal investigations, or where there is no indication of individual wrongdoing, an employee may not feel the need for counsel or may be happy working with company counsel. While joint representation by company counsel is often the most expedient and economical choice for employers, company counsel is not always the right choice for the client and ultimately may be problematic for the company. The opportunity for conflicts to arise in a joint representation is substantial, particularly where the client may give testimony contradicting the employer's position or creating liability for the employer.[85] For former employees, the risk of conflict is even more acute, as employee–employer interests are even less likely to be aligned. If clients elect not to co-operate, they will have no choice but to appoint independent counsel, owing to the inherent conflict created.[86]

A client may alternatively choose to appoint pool counsel, wherein the client is represented along with several other clients by one counsel. Pool counsel is an efficient way to provide representation for multiple employees while saving time and resources. It is typically appropriate when the clients are fact witnesses with minimal or no personal exposure, or fall into the same category (e.g., former employees); the subject of the interviews is likely to be similar; or the investigation is expected to be finite. Pool counsel is not appropriate when clients may contradict or give testimony creating liability for one another. Pool counsel must vigilantly monitor for conflicts and ensure that each client is aware of the duty owed to the others. To this end, clients should be counselled about the potential conflicts and

85 See also Model Rules of Prof'l Conduct r. 1.13 cmt. (Am. Bar Ass'n 2018) (providing that investigating counsel should advise employees whose interests may be adverse to the corporation that he or she 'may wish to obtain independent representation').

86 Counsel should also bear in mind that US authorities may take a dim view of joint representation, questioning the independence of the client's testimony or, at the most extreme, alleging that a conflict has arisen and insisting that independent counsel be retained.

See Chapter 16 on representing individuals in interviews

privilege implications[87] of pool counsel, and engagement letters should require clients' informed consent to the arrangement.[88]

Regardless of the type of counsel selected, clients should also consider whether to engage specialised counsel, such as employment counsel to advise on co-operation obligations under applicable labour law or employment agreements, or counsel specialising in the law of the foreign jurisdiction, for example in jurisdictions with stringent privacy laws or circumscribed attorney–client privilege protections.

18.4.5 Impact of company settlement

Counsel must consider the impact of a company's settlement or plea agreement, which may name individual employees, reference employee conduct or admit facts implicating individual employees. The risk that a company names individual employees is particularly acute given the DOJ's policy requiring companies to report misconduct by individual wrongdoers to receive co-operation credit. Counsel should advise clients that a company's settlement or plea agreement with enforcement authorities does not necessarily extinguish potential criminal liability for the client, nor does it eliminate the potential for claims in separate civil litigation, for example a shareholder derivative suit.

See Chapters 10 on co-operating with authorities, 24 on negotiating global settlements and 34 on parallel civil litigation

87 While '[a]n employee's cooperation in an internal investigation alone is not sufficient to establish a common interest', the privilege will be deemed waived where there is 'some form of joint strategy' among the parties. *In re Grand Jury Subpoena: Under Seal*, 415 F.3d 333, 341 (4th Cir. 2005) (quoting *United States v. Weissman*, 195 F.3d 96, 100 (2d Cir.1999)); see also *United States v. Aramony*, 88 F.3d 1369, 1392 (4th Cir. 1996) ('To be entitled to the protection of this privilege the parties must first share a common interest about a legal matter.'). Furthermore, it has become increasingly common for companies to include in joint defence agreements language that expressly allows the company to unilaterally disclose joint defence materials and information to other parties to the representation. See Ed Magarian and Surya Saxena, 'Joint Defense Agreements: What Is A Responsible Company To Do?', 22 Andrews Corp. Officers and Directors Liability Litig. Rep., September 2008, at 1 (2008).

88 In both pool and company counsel representations, counsel will need to obtain the client's consent to disclose confidential information to others in the pool and 'use' such information for the benefit of other clients (while maintaining the privilege to outside parties) under the joint defence privilege. Engagement letters also should clearly explain that pool counsel may use information provided by one client to zealously represent all clients in the pool (though information identified by a client as being confidential will only be shared with express authorisation). Relatedly, clients should be advised not to speak with any third parties about the substance of the investigation to preserve the integrity of the respective clients' recollections, and also because those communications will not be protected by the common interest or joint defence privilege. See, e.g., *United States v. Austin*, 416 F.3d 1016, 1021 (9th Cir. 2005) (joint defence privilege protects the confidentiality of communications 'passing from a party to his or her attorney' and 'from one party to the attorney for another party', but only 'where a joint defense effort or strategy' exists) (quoting *United States v. Schwimmer*, 892 F.2d 237, 243 (2d Cir. 1989)).

Evidentiary issues 18.5

Privilege laws across jurisdictions 18.5.1

A key consideration in cross-border proceedings is whether legal communications will be protected from disclosure to regulators and other parties. While in the United States these communications are protected by the attorney–client and work-product privileges, analogous protections are not always available in foreign jurisdictions.[89]

Additionally, in certain circumstances, US counsel's own communications with a foreign client may not be protected under US law. To determine whether such communications are privileged, US courts apply the 'touch base analysis', deferring to the privilege laws of the country with the 'predominant' or 'most direct and compelling interest'.[90]

Privilege protections may also diverge among jurisdictions with respect to communications with in-house counsel, an issue that typically arises in internal investigations. Under US federal law and the laws of each state, the attorney–client privilege applies equally to communications with external and in-house counsel.[91] In many European countries, however, the equivalent privilege applies only to written communications between clients and external counsel.[92]

Foreign privilege rules have a meaningful impact on the scope of materials and information available to investigating authorities and even counsel. It is therefore prudent to consult with local counsel to understand the scope of protections in the relevant jurisdiction.

---

89 In China, for example, there is no doctrine of legal privilege. Richard Bartlett and Yuan Min, A Lawyer's guide to working in China, King & Wood Mallesons (15 November 2017), https://www.kwm.com/en/knowledge/insights/a-lawyers-guide-to-working-in-china-20171113. And while the European Union provides for the 'legal professional privilege', it is comparatively limited, covering only counsel who are admitted to the bar in one of the Members States of the European Union. Patrick Doris and Steve Melrose, Privilege: European Union, Global Investigations Review. (12 October 2018), https://globalinvestigationsreview.com/preview_jurisdiction/1005270/european%20union?preview=1000391.

90 *Cadence Pharm., Inc. v. Fresenius Kabi USA, LLC*, 996 F. Supp. 2d 1015, 1019 (S.D. Cal. 2014). The country with the 'predominant interest' is either 'the place where the allegedly privileged relationship was entered into' or 'the place in which the relationship was centered at the time the communication was sent.' Id.

91 See, e.g., *Swidler & Berlin v. United States*, 524 U.S. 399, 408 (1998); see also Doug Gallagher, Manasi Raveendran, Attorney–Client Privilege for in-House Counsel, Am. Bar Ass'n (2017), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2017-18/november-december/attorney-client-privilege-inhouse-counsel/. Privilege issues arise more often in the context of communications with in-house rather than external counsel because, for example, in-house counsel may often play the dual role of offering both legal and business advice.

92 Ava Borrasso, Privilege and International Implications against the Backdrop of the Panama Papers, Am. Bar Ass'n (20 July 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/07/12_borrasso/.

18.5.2 Foreign restrictions on information transfer

Many countries have data protection laws restricting extraterritorial transfer of personal and corporate information. The General Data Protection Regulation (GDPR), which came into force in 2018, effected significant changes in data privacy.[93] The data protection and transfer laws of some countries further restrict how data can be shared or used.[94]

The practical effect is that counsel may not be able to transfer data to the United States and will need to review relevant material in a foreign jurisdiction.[95] Similarly, there may be restrictions on the materials or information a client can disclose to US authorities in interviews or productions. Clients (and counsel) could expose themselves to sanctions for failing to comply with these regimes[96] and should consult local counsel to ensure compliance.

See Chapter 40 on data protection and Chapter 12 on production of information to authorities

18.5.3 Evidentiary considerations in internal investigations

In internal investigations, clients may be asked to provide documents, emails or other records to company counsel. Clients typically must comply if the materials were created or maintained in the course of employment, as they are considered the employer's property.[97] Failure to comply risks disciplinary action, termination

93 The GDPR imposes certain obligations on individuals, organisations and companies who are 'controllers' or 'processors' of personal data and restricts how they may process and transfer that data. If the controller or processor wishes to transfer the data to a country the European Commission has not deemed adequate, such as the United States, it must identify whether a sufficient basis, or 'derogation', applies under the GDPR and implement safeguards to ensure GDPR compliance. One such derogation applies when the transfer is necessary for the establishment, exercise or defence of legal claims, which commonly applies in the context of criminal or other regulatory investigations, where transfer of data is necessary for the purpose of defending the individual client. See European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 11 (25 May 2018), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

94 See, e.g., Schweizerisches Strafgesetzbuch (Swiss Criminal Code), 21 December 1937, art. 349.

95 See, e.g., Loi 80-538 du 16 juillet 1980 relative à la communication de documents et renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères (Law 80-538 of 16 July 1980 Relating to the Communication of Economic, Commercial or Technical Documents or Information to Foreign Natural or Legal Persons), Journal Officiel de la République Française, 17 July 1980, art. 1A (Fr.).

96 See, e.g., Swiss Criminal Code 21 December 1937, SR 757 (1938), as amended by Gesetz, 4 October 1991, AS 2465 (1992).

97 The law is not entirely settled on this issue. The critical inquiry is whether (1) the materials were created or maintained in the course of employment, and (2) the employee had a reasonable expectation of privacy with respect to the materials. See, e.g., *Smyth v. Pillsbury Co*., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (no reasonable expectation of privacy in email communications made voluntarily over company email system even where employer told employees electronic communications would be kept confidential); but see *Levanthal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001) (public employee had reasonable expectation of privacy in contents of office computer because, inter alia, employee occupied private office with closed door and had exclusive use of desk, filing cabinet and computer); *Kellher v. City of Reading*, No. CIV.A.01-3386,

or being reported to authorities as unco-operative or obstructionist.[98] For this reason, too, clients should be counselled to carefully abide by any legal holds. Even if a hold has not issued, clients should preserve all potentially relevant materials to avoid even the appearance of potential spoliation.[99]

Notwithstanding the above, former employees may be able to assert the Fifth Amendment in refusing to produce incriminating documents to US authorities.[100] Current employees generally do not have this right.[101] Before turning over any documents to company counsel that may be shared with authorities, counsel should seek advice from local counsel regarding the client's (and counsel's) exposure for doing so under applicable data privacy or other local laws.

Finally, in most internal investigations, individual counsel is dependent on company counsel to obtain relevant materials. To this end, a cordial and co-operative relationship with company counsel is critical to facilitate information sharing.

See Chapter 16 on representing individuals

Asset freezing, seizure and forfeiture 18.6

Counsel should advise clients regarding the potential for asset freezing, seizure or forfeiture. In criminal proceedings, the DOJ may pursue criminal or civil forfeiture of tainted assets, that is, property derived from the criminal conduct, or substitute assets up to an equivalent value, if tracing the directly forfeitable property is impossible or the tainted assets are no longer available.[102] Criminal forfeiture

2002 WL 1067442, at *1 (E.D. Pa. 29 May 2002) (acknowledging that employee may have reasonable expectation of privacy in certain company email communications depending on the communication at issue and configuration of the relevant email system).

98 Note, however, that the client may have a cognisable claim that the materials are protected by the attorney–client or other applicable privilege. See e.g., *Sims v. Lakeside School*, No. C06-1412RSM, 2007 U.S. Dist. LEXIS 69568 (W.D. Wash. 20 September 2007).

99 Even where a company has not requested materials, it is prudent to advise clients to preserve any emails, notes or other documents that they believe may bear on the investigation. To assure adequate preservation, it may be necessary to engage a reputable third-party forensic technician to image or otherwise preserve the documents or data in question.

100 Former employees may claim an 'act of production' privilege in refusing to produce documents 'where the act of production is, itself, (1) compelled, (2) testimonial, and (3) incriminating.' *In re Three Grand Jury Subpoenas Duces Tecum Dated Jan. 29, 1999*, 191 F.3d 173, 178 (2d Cir. 1999). It is not clear, however, how a court might rule where the documents in the former employee's possession are deemed to be the company's property, e.g., where the employee took the documents upon leaving the employer without permission and/or in violation of company policy. But see id. at 182-83.

101 In *Braswell v. United* States, 487 U.S. 99, 102 (1988), the Supreme Court held that current employees may not claim the act of production privilege, even if those documents are incriminating against the employee, because the employee is an agent of the company and the records were in the employee's custody in his capacity as an agent. The Court did not address whether the outcome might differ if the records in question were personal to the employee or not maintained in his capacity as an agent of the company. In light of *Connolly*, former employees in an internal investigation conducted at the behest of the government might have an argument that the act of production privilege applies to them as well.

102 See, e.g., 18 U.S.C. §§ 981, 982; 21 U.S.C. § 853.

charges must be included in the indictment.[103] A criminal forfeiture order typically cannot be obtained unless the client is criminally convicted of, or has pleaded guilty to, a forfeiture offence.[104] In civil proceedings, the DOJ must file an *in rem* action, namely one against the property derived from or used to perpetrate the crime,[105] and usually seizes the property (with the exception of real property) before the court's entry of a civil forfeiture order.[106]

The DOJ also may obtain a pre-indictment or pretrial restraining order to freeze assets that have not yet been seized.[107] The SEC may similarly freeze assets through a temporary pretrial restraining order to ensure that funds for a future disgorgement order are available.[108]

If the assets subject to forfeiture are unavailable as a result of the client's act or omission, US authorities can satisfy the forfeiture order through substitute assets (other assets of the client of comparable value).[109] Counsel should discuss with clients the impact this may have on joint assets such as a home or other property shared with a spouse.[110]

See Chapter 31 on individual penalties

US authorities have increasingly sought to freeze and seize assets in white-collar cases involving securities fraud, bribery, money laundering and insider trading, even when the assets in question are located outside the United States.[111] 2019 was no exception to that trend.[112]

103 See Fed. R. Crim. P. 32.2(a).

104 See 18 U.S.C. §§ 982(a), 1963(e); Fed. R. Crim. P. 32.2(b)(1)(A).

105 See 18 U.S.C. §§ 983(a)(4), 984(a)(1), 985(c); see also 18 U.S.C. § 983(a)(1); 19 U.S.C. § 1607.

106 Id. § 985(b)(1).

107 Id. § 983(j). The government must have probable cause to believe the property constitutes proceeds of crime or was used during the commission of a crime. See 21 U.S.C. 853(e)(2). An indictment returned by a proper grand jury 'conclusively determines the existence of probable cause'. *Kaley v. United States*, 571 U.S. 320, 328 (2014) (citing *Gerstein v. Pugh*, 420 U.S. 103, 117 n.19 (1975)).

108 *SEC v. One or More Unknown Traders in the Securities of Onyx Pharmaceuticals, Inc.*, 296 F.R.D. 241, 254 (S.D.N.Y. 2013) (citing SEC v. Unifund SAL, 910 F.2d 1028, 1041 (2d Cir. 1990)).

109 21 U.S.C. § 853(p).

110 See, e.g., *United States v. Butler*, 543 F. App'x 95, 97 (2d Cir. 2013).

111 The United States is a party to a number of treaties, as well as other formal and informal agreements, that provide for freezing or seizure of assets in foreign jurisdictions. See, e.g., U.S. Internal Revenue Service, Internal Revenue Manual § 9.7.10.1.2 (28 July 2003), https://www.irs.gov/irm/part9/irm_09-007-010#idm140235861363504. In addition, US authorities (and private civil litigants) may register seizure or forfeiture orders issued by US courts in foreign jurisdictions in hopes of enforcing those judgments abroad. See, e.g., Mutual Legal Assistance Treaty, U.S.-U.K., art. 19(2) 6 January 1994, T.I.A.S. No. 96-1202.

112 For example, in 2019, the DOJ announced the filing of a third round of civil forfeiture complaints in the 1MDB prosecution, bringing the total seizure amount over $1.5 billion. See U.S. Dep't of Justice press release, 'Former Banker Extradited from Malaysia to United States to Face Charges in Multi-Billion Dollar Money Laundering and Bribery Scheme Relating to the 1MDB Fund' (6 May 2019), https://www.justice.gov/opa/pr/former-banker-extradited-malaysia-united-states-face-charges-multi-billion-dollar-money; see also supra note 61.

Collateral consequences 18.7

Counsel must be attuned to numerous collateral consequences of a cross-border proceeding. These include the potential for (1) parallel actions by other authorities (domestic or foreign), (2) follow-on civil litigation by shareholders or victims, (3) revocation or suspension of regulatory or professional licences or registrations, (4) difficulty obtaining requisite background or 'know your customer' clearance for employment or personal finances, (5) reputational harm and (6) immigration or travel consequences, particularly if the offence is deportable or where extradition has been defeated.

The human element: client-centred lawyering 18.8

Individual representations raise unique issues concerning client-centred lawyering beyond those that typically arise in a corporate representation. Criminal actions are particularly traumatic for both clients and their families, particularly given that most white-collar clients are interacting with the criminal justice system for the first time. While the luxury of time is not always available, counsel should strive to allow the client enough of it to process the situation before making any irreversible decisions.

Counsel also must be attuned to the impact of the proceeding on the client's physical and mental health. Preliminary discussions should cover these issues, as well as the client's support system. Engaging with the client's support system is essential at all stages, including fact gathering, assessing strategic options, deploying financial resource and determining resolution. For clients facing criminal proceedings, family support impacts all aspects of the case, from bail conditions to the sentence imposed.

Finally, counsel must be sensitive to the impact of the proceeding on the client's professional and personal reputation. Even if no enforcement action is taken, mere association with a proceeding – particularly if criminal – may so negatively impact the client's reputation that he or she is unable to work in the industry again or live in the same community.[113] Counsel should be prepared to advise clients on how to mitigate reputational risks and expect that these considerations will impact clients' decisions.

See Chapter 38 on publicity

113 Reputational concerns are likely to be heightened when the proceeding is high profile and the client faces media inquiries. While clients may wish to hire a public relations firm, any decision to engage a third party should be carefully considered in light of the fact that those communications are often not privileged and could adversely affect the outcome of the proceeding. See, e.g., *Haugh v. Schroder Inv. Mgmt. N. Am. Inc.*, 02-7955, 2003 WL 21998674, at *3 (S.D.N.Y. 25 August 2003).

19

Whistleblowers: The UK Perspective

Jillian Naylor, Alison Wilson, Sinead Casey and Elly Proudlock[1]

19.1 Introduction

Recent years have seen an increasing focus on whistleblowing as a cornerstone of good corporate culture. By helping to uncover wrongdoing or errors within an organisation, effective whistleblowing procedures are integral to good governance and risk management. They allow problems to be identified early, providing an opportunity to rectify shortcomings and to prevent a crisis. Being aware of issues also allows businesses to manage market-notification obligations and public relations, identify poor performance and potentially avoid costly employment litigation.

The focus on whistleblowing as fundamental to good governance has been particularly evident in the financial sector, where a key feature of the Senior Managers and Certification Regime (SMCR) is a requirement for firms to appoint a 'whistleblowers' champion'. However, the role of whistleblowing has also been the subject of scrutiny outside the regulated sector. For example, a 2015 report into whistleblowing in the National Health Service (NHS) provoked a series of reforms aimed at ensuring that speaking up becomes 'business as usual' within the NHS. A principal aim of those reforms was to mirror the open reporting culture in other safety-critical sectors, most notably aviation.[2]

---

1 Jillian Naylor, Alison Wilson and Sinead Casey are partners, and Elly Proudlock is counsel at Linklaters LLP. The authors wish to acknowledge the contribution of Peter Binning, a partner at Corker Binning, and Elisabeth Bremner, a partner at CMS Cameron McKenna Nabarro Olswang LLP, for their contributions to a previous version of this chapter.

2 Freedom to Speak Up, Sir Robert Francis QC, February 2015. See http://freedomtospeakup.org.uk/wp-content/uploads/2014/07/F2SU_web.pdf.

While there is no general obligation on workers to disclose wrongdoing, certain categories of employee – particularly those in the regulated sector – may have specific reporting obligations to their employers or regulators. The Employment Rights Act 1996 (ERA), as amended by the Public Interest Disclosure Act 1998 (PIDA), provides protection to workers who blow the whistle by protecting them against detrimental treatment and (in the case of employees) from being dismissed for making certain specified types of 'qualifying protected disclosures'. Compensation for successful Employment Tribunal whistleblowing claims is uncapped. Such legal protections relate only to dismissal or detriment in an employment context and do not provide immunity from criminal prosecution where a whistleblower is implicated in criminal conduct.

Outside the financial services sector, there is currently no requirement for organisations in the United Kingdom to have whistleblowing mechanisms. However, the EU Directive on the protection of persons reporting on breaches of Union law (the Whistleblower Directive) was formally adopted in October 2019. Among other measures, the Directive – which Member States have until October 2021 to implement – will require organisations with 50 or more employees to establish internal reporting channels and respond to reported concerns within three months.[3] In addition, in July 2019 a report of the All Party Parliamentary Group (APPG) for Whistleblowing recommended the introduction of mandatory internal and external reporting mechanisms along with meaningful penalties for those who fail to meet the requirements across all sectors.[4]

The APPG has also urged the government to ban the use of non-disclosure agreements (NDAs) in whistleblowing cases.[5] The use of NDAs in settlements with employees has attracted considerable media attention in the wake of the #MeToo movement.[6]

The legal framework 19.2

Public Interest Disclosure Act 1998 and Employment Rights Act 1996 19.2.1

Whistleblowing legislation was introduced in 1998 following the realisation that a number of high-profile disasters may have been prevented or their effect reduced

3 Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting on breaches of Union law. Whether the United Kingdom remains under such an obligation will depend on the terms of its anticipated departure from the European Union.

4 See https://www.appgwhistleblowing.co.uk/.

5 Ibid., Recommendation 7 in the '10 Point Plan'.

6 See, for example, 'British #MeToo scandal' puts non-disclosure agreements in spotlight, *The Guardian*, Esther Addley and Dan Sabbagh, published 24 October 2018 (https://www.theguardian.com/world/2018/oct/24/british-metoo-scandal-puts-non-disclosure-agreements-in-spotlight) and NDAs: The Cause Of #metoo?, *Forbes*, Sarah Chilton, published 24 February 2019 (https://www.forbes.com/sites/sarahchilton/2019/02/24/ndas-the-cause-of-metoo/#7194cfc02de5).

if a worker had spoken up, or their employer had listened to them.[7] PIDA came into force in July 1999, inserting new sections into ERA. PIDA provides two key protections: unlawful detriment (protecting employees and workers, including some LLP members[8]) and automatically unfair dismissal (protecting employees). There is no qualifying length of service for bringing whistleblowing claims.

19.2.1.1 Unlawful detriment

Subjecting a worker to a detriment because they have made a protected disclosure is unlawful. Detriments include, but are not limited to, pay cuts, limiting career prospects and disciplinary action. Detriments after termination of employment also qualify,[9] so employers should proceed cautiously when drafting references.

19.2.1.2 Automatically unfair dismissal

Dismissing an employee who has blown the whistle is automatically unfair if the reason, or principal reason, for the dismissal is that they have made a protected disclosure. Since compensation for successful whistleblowing unfair dismissal claims is uncapped, compensation can be high – especially if the individual encounters difficulty finding a new job because of the dismissal.

19.2.1.3 Qualifying disclosures

Six categories of disclosure are protected as 'qualifying disclosures'. The disclosure must, in the worker's reasonable belief, tend to show that one or more of the following failures has occurred or is likely to occur:

- a criminal offence;
- breach of a legal obligation;
- a miscarriage of justice;
- danger to the health and safety of any individual;
- damage to the environment; or
- the deliberate concealment of information about any of the above.

Since 2013, to make a qualifying disclosure the worker must reasonably believe that the disclosure is in the public interest.[10] 'Public interest' is not defined, but in *Chesterton Global and Verman v. Nurmohamed*,[11] the Court of Appeal decided that the interests served by the disclosure do not have to extend outside the workplace. The Court found that four considerations are relevant:

- the number of people affected by the disclosure;

7 For example, the Zeebrugge ferry disaster in 1987, the Clapham rail crash in 1988 and the BCCI collapse in 1992.

8 In C*lyde & Co LLP v. Bates van Winkelhof* (2014) UKSC 32, the Supreme Court held that a former equity partner of a law firm incorporated as a limited liability partnership (LLP) was a worker under section 230(3) of ERA and therefore eligible to bring a whistleblowing claim against the LLP.

9 *Woodward v. Abbey National Plc* (2006) EWCA Civ 822.

10 Section 17 of the Enterprise and Regulatory Reform Act 2013 amended ERA at section 43B(1).

11 (2017) EWCA Civ 979.

- the nature of the interests affected;
- the extent to which those interests are affected; and
- the identity of the alleged wrongdoer.

Anything that affects a class of people could potentially be caught, so employers should take a cautious approach. It is possible that 'everyday' employment disputes over contractual terms will have a public interest element, especially where these have serious implications or impact large numbers of people (for instance, remuneration issues in public limited companies and financial institutions). Issues such as discrimination or equal pay at work might also have a public interest element.

So long as the worker believes, acting reasonably, that the relevant failure has occurred or is likely to occur, they will be protected even if their belief turns out to be wrong.[12] However, for a belief to be 'reasonable' it must be founded in more than unsubstantiated rumour or opinion.

Since 2013, there is no longer any requirement for the disclosure to be 'in good faith'. However, if an employment tribunal upholds an employer's argument that a disclosure was made in bad faith, it has the power to reduce compensation by up to 25 per cent. Case law suggests that disclosures made predominantly for personal interest or with malice are not in good faith.[13]

Vicarious and personal liability 19.2.1.4

Vicarious liability

In June 2013, the Enterprise Regulatory and Reform Act 2013 introduced the concept of vicarious liability into whistleblowing law. It imposes vicarious liability on an employer for detriments caused to a worker by co-workers (and in some cases by agents of the employer) on grounds that the worker made a protected disclosure.[14]

The employer will have a defence if it took all reasonable steps to prevent the detrimental treatment. Having an appropriate whistleblowing policy and providing training to support this will be key to an employer's ability to evidence this.

Personal liability

Claimants can pursue individuals personally for liability arising from whistleblowing detriments. Doing so is often tactical. In *Timis and another v. Osipov*,[15] the employment tribunal and Employment Appeal Tribunal held that two non-executive directors were jointly and severally liable for the losses flowing from Mr Osipov's dismissal (totalling approximately £1.75 million).

12 *Babula v. Waltham Forest College* (2007) EWCA Civ 174.

13 *Bachnak v. Emerging Markets Partnership Europe* (2006) UKEAT/0288/05/RN.

14 Enterprise and Regulatory Reform Act 2013, section 19.

15 [2018] EWCA Civ 2321.

19.2.2 EU Directive and UK implementation

In October 2019, the Council of the European Union formally adopted the Whistleblower Directive.

Since the United Kingdom already grants whistleblowers comprehensive protection, for the most part the provisions of the Whistleblower Directive do not supplement the whistleblower protection already available under the UK domestic legislation. However, the following differences should be noted:

- organisations with 50 or more employees will be required to establish internal reporting channels for the reporting of breaches of Union law, to acknowledge receipt of a report within seven days and to respond to reported concerns within three months; and
- whistleblowers will also have the right to make an external disclosure to a competent national authority or, in limited cases, a public disclosure.

Member States have until October 2021 to implement the Directive. Whether the United Kingdom remains under such an obligation will depend on the terms of its anticipated departure from the European Union. Protect,[16] the whistleblowing charity, has urged the UK government to bring the new provisions into domestic law post-Brexit.

19.2.3 Non-disclosure agreements and whistleblowing

An NDA – a contractual commitment that a party (or parties) will keep certain information confidential – is a provision commonly included in settlement agreements between employers and departing employees. Under an NDA, confidentiality may attach to the terms of the settlement agreement and to the amount of any sums paid under it, as well as to the underlying complaints that the employee made. If the NDA is breached, the other party can seek damages for breach of contract.

In the wake of the #MeToo movement, the use of NDAs by employers has come increasingly under the spotlight and has been criticised, in particular, as a means of silencing whistleblowers. In July 2019, the APPG for Whistleblowing urged the government to ban the use of NDAs in whistleblowing cases.[17]

Any NDA clause designed to prevent a worker from making a whistleblowing disclosure is void under section 43J of ERA and therefore unenforceable. Seeking to rely on an NDA to prevent whistleblowing disclosures could amount to an unlawful detriment against the employee or worker, as well as risking additional adverse publicity if the issue becomes public.

See Sections 19.2.4 and 19.4.3

Firms authorised by the Financial Conduct Authority (FCA) are under specific obligations when it comes to settlement agreements with workers. Lawyers advising clients on NDAs must also consider their professional obligations.

16 Previously known as Public Concern at Work. See https://protect-advice.org.uk/.

17 See https://www.appgwhistleblowing.co.uk/.

FCA/PRA systems and controls requirements 19.2.4

Both the FCA and the Prudential Regulation Authority (PRA) expect firms to implement and maintain appropriate and effective internal whistleblowing arrangements as part of an effective risk management system.[18] The FCA's rules and guidance are contained in SYSC 18 of its Handbook, which applies to SMCR banking and insurance sector firms. SYSC 18 also serves as non-binding guidance to all other firms authorised under the Financial Services and Markets Act 2000 (FSMA). The PRA's rules are higher level and found in Section 2A of the PRA Rulebook.

The SYSC 18 requirements fall into three categories:

- maintenance of appropriate and effective arrangements for whistleblowing;[19]
- appointment of a whistleblowers' champion;[20] and
- settlement agreements with workers.

Maintaining appropriate internal whistleblowing arrangements 19.2.4.1

While firms are required to establish, implement and maintain appropriate and effective arrangements for the disclosure of reportable concerns (including concerns related to suspected market abuse) by whistleblowers, neither regulator has prescribed what the arrangements should be. FCA guidance suggests that firms may choose to draw on relevant resources prepared by whistleblowing charities or recognised standards-setting organisations, such as Protect. The regulators recognise that whistleblowing arrangements may vary between firms[21] and that firms may use third parties to provide aspects of their whistleblowing services, with appropriate quality controls and monitoring.

The arrangements that a firm has in place should allow effective escalation of reportable concerns, including to the FCA and PRA. This requirement is aligned with PRA Fundamental Rule 7 and FCA Principle 11, according to which firms must deal with their regulators openly and co-operatively and disclose appropriately anything relating to the firm of which the regulators would reasonably expect notice. Beyond these broad principles, a firm's arrangements should:

- allow for disclosure to be made through a variety of means (for many firms this will mean through an online system, a telephone hotline, a third-party provider or a designated team);
- handle a whistleblower's request for confidentiality or anonymity;
- include reasonable measures to ensure whistleblowers are not victimised;
- provide feedback to whistleblowers on their concerns, where appropriate and feasible;
- include record-keeping of reportable concerns;

18 FCA Handbook, SYSC 18.3.1(1)R; PRA Rulebook Whistleblowing 2A.2(1).

19 FCA Handbook, SYSC 18.3.

20 FCA Handbook, SYSC 18.4.

21 Whistleblowing in deposit-takers, PRA designated investment firms and insurers – SS39/15 (Supervisory Statement, October 2015, updated July 2018).

- include maintenance of up-to-date whistleblowing policies and procedures that are readily available to the firm's employees;
- allow for the preparation of an annual report to the firm's governing body on the effectiveness and operation of the firm's processes;
- include training for employees, managers and those responsible for operating the firm's internal arrangements;
- include reporting to the FCA and PRA if firms lose an employment tribunal claim based on detriment suffered from making a protected disclosure; and
- ensure UK employees are made aware of the FCA's and PRA's whistleblowing services and that they can approach either regulator direct without first raising a concern internally.

19.2.4.2 The whistleblowers' champion

A key component of the SMCR is a requirement for firms to appoint a whistleblowers' champion with responsibility for ensuring and overseeing the integrity, independence and effectiveness of the firm's policies and procedures on whistleblowing. The FCA expects that this role will be filled by a non-executive director.[22] Assignment of specific responsibility for whistleblowing to a senior person – preferably the chairman – was a recommendation of the June 2013 report of the Parliamentary Commission on Banking Standards, Changing Banking for Good, and is consistent with the broader trend towards senior management responsibility in the UK regulatory regime. This is reflected both in the fact that the whistleblowers' champion is now a prescribed responsibility under the SMCR,[23] and in the guidance that the whistleblowers' champion should have a level of authority within the firm sufficient to carry out their function.[24]

The whistleblowers' champion is also expected to ensure that an annual report is presented to the board regarding the effectiveness of whistleblowing systems and controls. The FCA and PRA have not been prescriptive about how whistleblowers' champions perform their role, and have acknowledged that firms are likely to take different approaches depending on their structure and size.[25] In smaller firms, the whistleblowers' champion may choose to take a 'hands-on' role, possibly in concert with his or her support staff, receiving disclosures personally and taking responsibility for disseminating reports within the firm, tracking progress, making external reports, feeding back to whistleblowers where appropriate and reviewing settlement agreements. In larger firms, whistleblowers' champions are more likely to perform their function by delegating day-to-day operations to a dedicated whistleblowing function while retaining an oversight role. The PRA expects the whistleblowers' champion to have access to resources and information

22 FCA Handbook, SYSC 18.4.1(4)G.

23 FCA Handbook, SMF 13, see SYSC 24.2.6R.

24 FCA Handbook, SYSC 18.4.5(1)G.

25 Whistleblowing in deposit-takers, PRA designated investment firms and insurers – FCA CP15/4, PRA CP6/15 (FCA/PRA Consultation Paper, February 2015)

sufficient to carry out their role.[26] In practice this is likely to include a regular suite of management information on the number and outcome of reportable concerns, as well as analysis or oversight of patterns in data – for example particular business units or offices in respect of which reportable concerns are more frequently raised.

Settlement agreements with workers 19.2.4.3

The FCA's rules require a firm to include in a settlement agreement with a worker a term making clear that nothing in that settlement agreement prevents the worker from making a protected disclosure. [27]

Competition and Markets Authority and whistleblowers 19.2.5

In exceptional circumstances, the Competition and Markets Authority (CMA) offers rewards of up to £100,000 for information about cartel activity. The rewards are provided at the discretion of the CMA subject to factors including the value of the information, the harm done to consumers and the risk the whistleblower has taken to provide the information.[28]

The CMA also operates a leniency programme according to which businesses and individuals who have participated in cartel activity may apply for immunity or leniency from financial penalties and immunity from criminal prosecution and director disqualification.[29] Complete immunity from sanctions might be granted provided the individual or business is the first to report and confess their involvement, they co-operate fully and there was no pre-existing investigation by the CMA.

Companies or individuals thinking about applying for leniency may, before doing so, approach the CMA for confidential guidance on a no names basis by calling the dedicated CMA's cartels hotline.[30] On 22 October 2018, the CMA launched its nationwide 'Stop Cartels' campaign, designed to encourage whistleblowing.[31] Following its launch, tip-offs to the CMA have risen by over 30 per

26 Whistleblowing in deposit-takers, PRA designated investment firms and insurers – SS39/15 (Supervisory Statement, October 2015, updated July 2018).

27 FCA Handbook, SYSC 18.5.1R. A *pro forma* clause is provided in SYSC 18.5.2.

28 The CMA's published policy on rewards for information about cartels is available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/299411/Informant_rewards_policy.pdf.

29 For guidance on applications for leniency and no-action in cartel cases, see the CMA's Applications for leniency and no-action in cartel cases (OFT 1495, July 2013).

30 The CMA will give its views, by which it will consider itself bound, provided the discussion is followed-up by an application within a reasonable time and provided the information given when the advice was sought was not false or misleading and there has been no material change of circumstance.

31 See https://www.gov.uk/government/news/cma-sends-tough-message-to-business-cheats-with-cartel-campaign.

cent,[32] with approximately 22,000 people having visited the campaign page.[33] However, the CMA's whistleblowing statistics from 2017 to 2018 indicate that only 23 cases required initial investigation or further investigation by the CMA.[34]

19.2.6 Serious Fraud Office and online whistleblowing

The SFO launched its whistleblowing service in 2011. Originally established as a telephone hotline, reports are now made electronically to the SFO's Intelligence Unit through its secure reporting form.[35] The SFO reporting service enables companies' executives, staff, professional advisers and business associates to provide information about cases of serious fraud, bribery or corruption – whether as a whistleblower or on behalf of a company making a self-report. Whistleblowers are initially encouraged to follow the whistleblowing procedures in their own organisation if they suspect wrongdoing in the workplace. If the whistleblower is not comfortable, or there are no procedures, then they should approach the SFO or another prescribed body.[36]

See Chapter 3 on self-reporting to authorities

Between 1 April 2017 and 31 March 2018, the SFO's Intelligence Unit managed 102 qualifying[37] whistleblowing disclosures. The SFO took further action in relation to 91 disclosures.[38] However, the take-up of cases for investigation by the SFO remains low, with only 10 criminal investigations opened in 2018.[39] In considering whether to authorise an investigation, the Director of the SFO will take into account the actual or intended harm that may be caused to the public, the reputation and integrity of the United Kingdom as an international financial centre or the economy and prosperity of the United Kingdom.[40]

Although there are means to report online via the SFO or National Crime Agency (NCA) websites, no single centralised mechanism exists to report bribery offences. To address this, the Home Office has committed to launching a new reporting mechanism for allegations of bribery and corruption in line with the

32 Sean McNabb, 'Working with us to tackle cartels' (CMA, 9 August 2019). Available at https://competitionandmarkets.blog.gov.uk/2019/08/09/working-with-us-to-tackle-cartels/.

33 CMA, Annual Report and Accounts 2018/19, page 17. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818478/CMA_Annual_Report_and_Accounts_2018_19_web_accessible_proof.pdf.

34 https://www.gov.uk/government/publications/whistleblower-statistics-2017-to-2018/whistleblowing-statistics-2017-to-2018.

35 The 'Secure Reporting Form' is available at https://www.sfo.gov.uk/contact-us/reporting-serious-fraud-bribery-corruption/.

36 See https://www.sfo.gov.uk/publications/information-victims-witnesses-whistleblowers/#whistleblowers.

37 To qualify for inclusion in the report, a disclosure must relate to serious or complex fraud (including bribery or corruption), civil recovery of the proceeds of crime, civil recovery investigations or disclosure orders in relation to confiscation investigations.

38 See https://www.sfo.gov.uk/download/annual-report-on-whistleblowing-disclosures-2017-18/#.

39 Number of SFO Investigations, July 2019. Available at https://www.sfo.gov.uk/publications/corporate-information/freedom-of-information/.

40 See https://www.sfo.gov.uk/contact-us/reporting-serious-fraud-bribery-corruption/.

government's anti-corruption strategy.[41] How this will interact with existing reporting mechanisms remains to be seen.

Human rights considerations 19.2.7

Demonstrating respect for human rights is increasingly important for businesses. In recent years, there has been a proliferation of 'soft law' standards encouraging companies to manage more closely their human rights risks and impacts. The key development in this area were the UN Guiding Principles on Business and Human Rights (UNGPs),[42] around which there has been widespread business convergence since their endorsement by the UN in 2011. The UNGPs require that business enterprises 'respect human rights',[43] which means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.

While business and human rights was previously the domain of 'soft law' instruments, we are increasingly seeing laws that require companies to report on their human rights risks and impacts. For example, section 54 of the Modern Slavery Act 2015 requires companies with an annual turnover of £36 million or more to produce a slavery and human trafficking statement for each financial year, either illustrating the steps the organisation has taken to ensure slavery and human trafficking is not taking place in any of its supply chains and any part of its business or confirming that the organisation has taken no such steps. Similarly, section 414CA of the Companies Act 2006[44] requires certain large companies to prepare a non-financial information statement containing information on a company's respect for human rights and a description of policies pursued by a company in relation to respect for human rights.

Businesses have realised that, to fulfil their obligations to respect human rights under the UNGPs and report effectively pursuant to these disclosure regimes, they need to conduct more extensive due diligence on their operations to understand their potential human rights risks and impacts. A properly functioning whistleblower system should enable human rights impacts to be identified, managed and (hopefully) remediated early and completely, preventing harm from escalating. Many companies have implemented whistleblowing policies to support the

41 House of Lords, Select Committee on the Bribery Act 2010, Report of Session 2017–19, 'The Bribery Act 2019: post-legislative scrutiny'. Available at https://publications.parliament.uk/pa/ld201719/ldselect/ldbribact/303/303.pdf.

42 UN High Commissioner for Refugees, Guiding Principles on Business and Human Rights, 2011, available at https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf.

43 UNGP 11, ibid., p.13.

44 Inserted by The Companies, Partnerships and Groups (Accounts and Non-Financial Reporting) Regulations 2016 published in 2016 as part of the UK Government's implementation of Directive 2014/95/EU of the European Parliament, commonly known as the 'EU Non-Financial Reporting Directive' or 'NFRD'.

management of human rights and supply chain risk, which is recommended in Home Office guidance.[45]

While whistleblowing can serve as a tool for identifying potential human rights risks and impacts, it is important to recognise the potential human rights consequences if the whistleblowing procedures do not contain sufficient protections for the whistleblower. This includes impacts on the rights to privacy and freedom of speech, which are protected under Articles 8 and 10 of the European Convention on Human Rights. These human rights are qualified, in that they need to be balanced against the public interest (or indeed the corporate interest) in identifying where human rights impacts have occurred and where laws may have been broken. The regulatory regimes governing the design and implementation of whistleblowing procedures are designed to balance these competing interests. However, human rights considerations should underpin the design and operation of an effective whistleblowing regime and used to resolve any ambiguity in the regulation.

19.3 The corporate perspective: representing the firm

19.3.1 Responsibility for whistleblowing among senior managers under SMCR

When representing a regulated firm involved in a whistleblowing investigation, regard must be had both to the firm's compliance with the systems and controls requirements outlined above and to individual managers' personal obligations under the SMCR.

The SMCR requires most individuals employed in the UK banking and insurance sectors to adhere to the FCA's and PRA's Individual Conduct Rules.[46] Senior managers must also comply with the Senior Manager Conduct Rules, while non-executive directors (who are not themselves senior managers) are subject to Senior Manager Conduct Rule 4 as well as the Individual Conduct Rules. At the time of writing, the SMCR was due to be extended to certain other financial services firms, including asset management firms and non-bank mortgage lenders, from 9 December 2019.

Certain individual rules may require the relevant individuals to disclose information to the regulators. In the context of whistleblowing, this means that information received via internal whistleblowing channels may, in turn, need to be escalated to the appropriate regulator.

19.3.1.1 Individual Conduct Rules

The FCA/PRA Individual Conduct Rule 3 stipulates that relevant individuals must be open and co-operative with the FCA, the PRA and other regulators with

45 UK Home Office, 'Transparency in Supply Chains etc. – A practical guide', p. 29. available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/649906/Transparency_in_Supply_Chains_A_Practical_Guide_2017.pdf.

46 See Code of Conduct (COCON) 2.1, FCA Handbook.

appropriate jurisdiction. The FCA's Code of Conduct Handbook (COCON) provides specific guidance as to what this rule requires.

COCON 4.1.10 provides guidance that there is no duty on a person to report information directly to the regulator concerned unless they are one of the persons responsible in the firm for reporting matters to the regulator (although if a person takes steps to influence the decision not to report or acts in a way that is intended to obstruct the reporting of the information to the regulator, they will be treated as if they had taken on responsibility for deciding whether to report that matter).

Those operating a whistleblowing function will not therefore automatically assume direct responsibility for escalating reportable concerns to the regulator. However, firms should ensure that appropriate arrangements are in place so that those responsible for regulatory reporting are informed on a timely basis of issues likely to be of interest to the regulator identified through the whistleblowing channels.

Senior Manager Conduct Rules 19.3.1.2

The FCA/PRA Senior Manager Conduct Rule 4 requires senior managers and non-executive directors to disclose appropriately any information of which the FCA, PRA or other regulator with appropriate jurisdiction would reasonably expect notice (even where the regulator has not requested such information). While there is overlap between FCA/PRA Senior Manager Conduct Rule 4 and Individual Conduct Rule 3, COCON 4.2.26 makes clear that these are distinct obligations requiring proactive disclosure rather than just accurate responses to regulatory enquiries. COCON 4.2.28 clarifies that senior managers (or non-executive directors) need not report information outside the scope of their responsibility. However, once they become aware of the information (including through whistleblowing) they should make enquiries to satisfy themselves that it is being dealt with by the appropriate individual.

Approved persons 19.3.1.3

Until the SMCR is extended in December 2019, relevant individuals employed by firms outside the banking and insurance sectors will continue to be governed by the approved persons regime. Statement of Principle 4 of the Statements of Principle and Code of Practice for Approved Persons broadly reflects Senior Manager Conduct Rule 4, although the accompanying guidance differs slightly.[47]

Whistleblowing as part of adequate or reasonable systems and controls 19.3.2

Bribery Act 2010 and adequate procedures 19.3.2.1

Under section 7 of the Bribery Act 2010, a company can be criminally liable for failing to prevent bribery committed for its benefit by one of its associated persons.

See Chapter 28 on extraterritoriality

47 Statements of Principle are found in APER 2 and guidance in APER 3 and APER 4, FCA Handbook, Statements of Principle and Code of Practice for Approved Persons.

It is a defence for a company to show that it had adequate procedures in place designed to prevent bribery by its associated persons.[48] Guidance published by the Ministry of Justice suggests that such procedures are likely to include, among other measures, procedures for the reporting of bribery including 'speak up' or 'whistleblowing' procedures.[49]

19.3.2.2 Criminal Finances Act 2017 and reasonable procedures

Under sections 45 and 46 of the Criminal Finances Act 2017, a company can be criminally liable for failing to prevent the facilitation of UK or foreign tax evasion offences by its associated persons.

It is a defence for a company to show that it had reasonable prevention procedures in place. Guidance issued by HM Revenue and Customs (HMRC) suggests that such procedures are likely to include, among other measures, protection for whistleblowers (with no retribution).[50] In February 2019, HMRC launched an online reporting form for authorised representatives to self-report a failure to prevent the facilitation of tax evasion on the part of their organisation.

See Chapter 3 on self-reporting to authorities

19.3.3 Changing regulatory expectations

In November 2018, following its review of firms' whistleblowing arrangements in the retail and wholesale banking sector, the FCA published examples of good practice and areas for improvement with respect to policies and procedures, the role of the whistleblowers' champion and the annual whistleblowing report and training.[51]

The FCA noted that some firms had a clear policy and other arrangements for ensuring whistleblowers were protected against victimisation, both during and following an investigation. For example, one firm monitored employment records for 12 to 18 months after a reportable concern had been investigated, to identify victimisation. The FCA also commended firms that had a variety of reporting channels for employees to raise concerns, with one firm providing whistleblowers the option of giving their contact details to a third-party hotline provider instead of to the firm. In contrast, the FCA was concerned by incorrect statements on the part of some firms that employees must raise whistleblowing concerns internally before contacting the FCA.

Good practice observed in respect of the whistleblowers' champion and annual report included senior individuals being able clearly to articulate the importance of a 'speak up' culture; champions having a good understanding of their roles

48 Section 7(2) of the Bribery Act 2010.

49 Ministry of Justice, The Bribery Act 2010: Guidance, paragraph 1.7. Available at https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

50 Page 23. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672231/Tackling-tax-evasion-corporate-offences.pdf.

51 Retail and Wholesale Banking: review of firms' whistleblowing arrangements (first published 14 November 2018). Available at www.fca.org.uk/publications/multi-firm-reviews/retail-and-wholesale-banking-review-firms-whistleblowing-arrangements.

and responsibilities, including providing independent oversight; one champion contacting whistleblowers to determine whether they had suffered adverse consequences or victimisation; reviews of effectiveness of whistleblowing arrangements by either the second or third line of defence or through third-party whistleblowing organisations; and staff surveys to ensure that employees knew how to raise concerns. The FCA did, however, find firms whose annual reports lacked detail or were still under development.

Good practices observed by the FCA with respect to training included the provision by some firms of separate training for managers and investigation teams. In the FCA's view, this approach helped to ensure that managers were equipped to provide the necessary management and support to those raising concerns. Good firms also provided training to senior leadership teams, especially where they were involved in assessing reportable concerns. At the same time, the FCA noted that most firms needed to improve the content of their training.

In May 2019, the FCA published its industry feedback with respect to wholesale banking.[52] It identified several practices as examples of 'encouraging' whistleblowing initiatives implemented by firms, including:

- engagement by managers and staff directly with a whistleblower to understand fully what he or she would like to achieve and make a sustained effort to manage appropriately the whistleblower's expectations;
- outsourcing of analysis on all whistleblowing cases to ensure fair and confidential treatment;
- detailed end-to-end reviews of the process for whistleblowing events involving all disciplines (e.g. HR, legal, compliance, business heads) to make it more transparent, fairer and quicker;
- creation of a 24-hour, multilingual hotline for anonymous escalations; and
- discreet monitoring for a minimum of three years following a whistleblowing event, to ensure a whistleblower was not treated badly as a consequence of their disclosure.

The importance of ensuring that a firm's systems and controls afford protection to whistleblowers was highlighted in the FCA and PRA final notices issued to Mr James Staley, Chief Executive of Barclays Group, in May 2018. Mr Staley was fined £642,430 following his attempts to identify the author of an anonymous letter received by Barclays. The regulators concluded that Mr Staley had made serious errors of judgement and had not acted with integrity or due skill, care and diligence as required by the Individual Conduct Rules. They also found that he had acted unreasonably and risked undermining confidence in Barclays' whistleblowing policy and the protections it afforded. Before the final notices were issued, Barclays voluntarily and successfully applied to be subject to special requirements until the end of 2020, made under section 55L and 55M(5) of FSMA. Under these requirements, Barclays must report annually to the FCA

52 See 'Progress and challenges' Industry Feedback for 2018/2019 Wholesale Banking Supervision (FCA, May 2019).

and PRA detailing any whistleblowing cases involving allegations made against its senior managers and any cases where Barclays has sought to identify any anonymous whistleblowers. It is also required to provide attestations about the soundness of its whistleblowing systems and controls and senior managers' completion of annual whistleblower training.

As part of its continued focus on culture in financial services, the FCA is particularly interested where whistleblowing allegations are raised against those designated as senior managers or material risk takers, being those with the greatest potential to cause harm to a firm's customers or the markets in which it operates. A number of firms have undertaken to notify the FCA of such allegations immediately on receipt and before investigation.

Megan Butler, FCA Executive Director of Supervision – Investment, Wholesale and Specialists Division,[53] in correspondence with the Chair of the Women and Equalities Committee of the House of Commons, set out her views on firms' approach to handling of '#MeToo' or sexual harassment allegations. She confirmed that sexual harassment and other forms of non-financial misconduct (such as racial or homophobic harassment or bullying) can amount to a breach of the FCA's conduct rules, including the requirement to act with integrity, and that firms' whistleblowing arrangements should be able to deal appropriately with escalation of such concerns. She noted that the FCA would be 'especially interested if firms were systematically mishandling allegations or incubating a culture of sexual harassment'. Since the letter, the FCA has engaged directly with some firms to request that it be notified of whistleblowing allegations of sexual harassment or other forms of non-financial misconduct promptly – even before investigation. This raises challenges for firms in terms of how to ensure fairness towards senior individuals where as yet unsubstantiated allegations are received.

Outside the financial regulatory sector, listed companies are required under the UK Corporate Governance Code 2018 to ensure that members of the workforce can raise concerns in confidence (and anonymously if they wish). The board should ensure that arrangements are in place for the proportionate and independent investigation of such matters and for follow-up action.

Also of wider relevance, in July 2019 the APPG for Whistleblowing published its report on the UK whistleblowing regime. Among its ten recommendations for what it calls a 'radical overhaul' were the introduction of mandatory internal and external reporting mechanisms across all sectors, greater legal protections for whistleblowers and the creation of an Independent Office for the Whistleblower.[54]

53 Letter dated 28 September 2018, https://www.fca.org.uk/publication/correspondence/wec-letter.pdf.

54 See https://www.appgwhistleblowing.co.uk/.

Practical considerations 19.3.4

Effective reporting channels and protecting anonymity 19.3.4.1

A whistleblowing policy should detail the process of making internal disclosures and should be disseminated across the organisation through regular communications and training that encourage a 'speak up' culture. Small and medium-sized organisations might consider appointing a dedicated whistleblowing officer in order to foster an open working culture, whereas in larger organisations an anonymous whistleblowing hotline is likely to be more practical. Ideally there should be a range of channels through which disclosures can be made.

It is often the case that workers report concerns anonymously out of fear that they will be victimised should they be identified as raising such concerns. This raises broader considerations in relation to how employers foster a culture in which workers feel 'psychologically safe' to raise concerns openly. However, a 2013 report by the Whistleblowing Commission on the effectiveness of existing arrangements for workplace whistleblowing suggested that, if a worker raises a concern anonymously, the organisation should assess the anonymous information as best it can to establish whether there is substance to the concern and whether it can be addressed.[55] Employers should also be aware that attempts to identify whistleblowers may constitute a breach of the employer's obligations under the Data Protection Acts of 1998 and 2018 or the General Data Protection Regulation (GDPR).[56]

Conduct of the investigation 19.3.4.2

Internal investigations involving whistleblower allegations require particularly careful handling because of the reputational and employment law consequences that may follow if a whistleblower is not afforded the required legal protections. No investigation is the same, and the right approach will depend on the circumstances and facts. Isolated incidents of minor misconduct may be capable of investigation internally by a combination of the legal, human resources and internal audit functions, whereas allegations of systematic or potentially criminal conduct are more likely to require the assistance of external counsel. Where there is a whistleblower involved, it is often advisable to interview them at the start of the process – particularly if they are relatively junior. Consideration should be given as to whether to offer them independent legal representation.

See Chapter 5 on beginning an internal investigation

See Chapter 7 on witness interviews

Where possible the whistleblower should be kept informed about the progress of the investigation, although extreme care should be taken not to take any steps that might result in a loss of privilege or confidentiality. Expectations should be effectively managed and care taken not to promise outcomes that may not be deliverable. For example, there may be circumstances in which a whistleblower's

See Chapter 35 on privilege

55 The Whistleblowing Commission, Report on the effectiveness of existing arrangements for workplace whistleblowing in the UK (November 2013) (https://www.tuc.org.uk/sites/default/files/Whistleblowing%20Commission%20Report%20Final.pdf).

56 (EU) 2016/679.

desire to remain anonymous places constraints on the extent to which the allegations can be investigated.

19.3.4.3 Data protection

A whistleblowing process will inevitably involve the processing of personal data and so must comply with the GDPR. The United Kingdom takes a more relaxed approach to this issue than many other European jurisdictions, in part because of the statutory framework set out in PIDA. However, it is still important to ensure that the whistleblowing process, and any subsequent investigation, complies with the GDPR. Particular issues to consider include keeping the whistleblowing information secure and limiting access to it, setting an appropriate retention period, not collecting excessive amounts of personal data, being alert to the right of individuals to access a copy of their personal data and, at least in general terms, being transparent about the operation of the whistleblowing process.

See Chapter 40 on data protection

19.3.4.4 Interaction with regulatory obligations

Principle 11 / Fundamental Rule 7

Firms must deal with their regulators in an open and co-operative way and proactively disclose anything relating to the firm of which the regulators would reasonably expect notice. Information that comes to light via a whistleblowing report may therefore have to be escalated to the relevant authority. In accordance with the FCA's Supervision manual (SUP), firms must notify the FCA of matters having a serious regulatory impact. This includes, for example, any matter that could have a significant adverse impact on the firm's reputation.[57] As noted above, in the current regulatory climate there may be a regulatory expectation that whistleblowing reports against senior managers or allegations of serious sexual harassment or other forms of serious non-financial misconduct will be disclosed immediately. In other situations, it may be more appropriate for a firm to undertake an internal investigation before deciding whether notification to the regulator would be proportionate.

Proceeds of Crime Act 2002 (POCA)

Depending on the subject matter of the allegation, those in receipt of whistleblower reports will need to consider whether the information disclosed raises potential money laundering issues such that the reporting obligations under POCA are triggered (for those in the regulated sector) or it is otherwise necessary to seek a defence against money laundering from the NCA to deal with certain property.

See Chapter 3 on self-reporting to authorities

Particular considerations for listed companies

When receiving whistleblowing reports, listed companies should also have regard to their disclosure obligations under the Disclosure Guidance and Transparency

57 See SUP 15.3.1R.

Rules (DTR) and the Market Abuse Regulation (MAR).[58] In accordance with Section 2.2 DTR and Article 17(1) MAR, for example, listed companies must disclose inside information to the market as soon as possible. To determine whether the information constitutes 'inside information' for the purposes of DTR and MAR, however, it is likely that the firm will first have to undertake an internal investigation into the allegations.

Cross-border considerations 19.3.4.5

Exchange of information in relation to whistleblowers or disclosures

See Chapter 3 on self-reporting and Chapter 40 on data protection

Data protection issues will need to be considered in the context of any transfer of data overseas.

Territorial application of UK whistleblower legislation

Recent case law has determined that a tribunal can only hear a whistleblowing claim against a British employer brought by an employee working abroad if there is a stronger connection with Britain or British employment law than with the country in which they are working. In *Foreign and Commonwealth Office (FCO) v. Bamieh*,[59] the Court of Appeal held that an employment tribunal had no territorial jurisdiction to hear whistleblowing detriment claims brought by an FCO employee working in Kosovo against co-workers who were also employed by the FCO and working in Kosovo. The tribunal held that the focus should be on the relationship between the claimant and the co-workers rather than on the relationship between the co-workers and the employer. Moreover, the fact that the individuals concerned have a common employer is not sufficient to give the tribunal jurisdiction.

The individual perspective: representing the individual 19.4

Legal risks associated with whistleblowing 19.4.1

A decision to make a whistleblowing disclosure can have far-reaching consequences and requires a careful assessment of the legal risks. Despite the protections afforded by PIDA, whistleblowers may be exposed to the risk of criminal investigation or prosecution if they are personally implicated in the conduct disclosed. Those in regulated professions may be vulnerable to regulatory or disciplinary action by their regulators or professional bodies. Where the matter potentially spans more than one jurisdiction, individuals will need to bear in mind that different jurisdictions apply different standards in the protection of whistleblowers. Advice on local employment and possibly criminal laws should be sought where necessary.

See Section 19.2.1

Whistleblowers might also commit criminal offences in the course of obtaining information to support their disclosures. Such offences might include securing

58 See DTR, FCA Handbook, Disclosure Guidance and Transparency Rules sourcebook.

59 (2019) EWCA Civ 803.

unauthorised access to computer material,[60] unlawfully obtaining personal data,[61] unlawful interception of communications,[62] theft or even fraud. Whistleblowers may also be vulnerable to civil actions for breach of confidence.

19.4.2 Serious Organised Crime and Police Act 2005: immunity and leniency

Where an individual faces criminal liability, they may be able to obtain immunity from prosecution. Section 71 of the Serious Organised Crime and Police Act 2005 (SOCPA) empowers most criminal prosecutors to offer an individual immunity from prosecution by issuing a written immunity notice. However, this power is used rarely and only in very exceptional circumstances.

As an alternative, section 73 of SOCPA provides that if an offender pleads guilty and offers assistance to an investigator or prosecutor, the sentencing court may pass a reduced sentence to reflect that assistance.

The historic reluctance by the SFO to invoke these statutory tools may be set to change following the appointment of Lisa Osofsky as Director of the SFO in August 2018. Ms Osofsky has publicly expressed an intention to make greater use of the powers contained in SOCPA,[63] though it remains to be seen whether this is achievable. The level of co-operation required to qualify for leniency is onerous and the risks to the individual are significant, particularly in cross-border investigations where there remains a risk of prosecution overseas.

See Chapter 17 on individuals in cross-border proceedings

19.4.3 Professional obligations

Those in regulated professions may have a duty to report certain information to the appropriate regulator. For example, FCA/PRA Senior Manager Conduct Rule 4 requires senior managers and non-executive directors to disclose appropriately any information of which the FCA, PRA or other regulator with appropriate jurisdiction would reasonably expect notice.

See Section 19.3.1

In March 2018, the Solicitors Regulatory Authority (SRA) issued a warning notice to legal professionals in relation to the use of NDAs,[64] which sets out the obligations that exist when a law firm is considering an NDA with a person who has made a complaint about misconduct within a law firm, or when legal professionals are advising clients on NDAs with individuals. The warning notice recognises that NDAs, including with employees, can legitimately be used to protect commercial interests and confidentiality and, in some circumstances, reputation. It also recognises that NDAs can operate to the mutual benefit of both parties and that the warning notice and the SRA's Standards and Regulations (replacing

60 Section 1 of the Computer Misuse Act 1990.

61 Sections 170 and 196 of the Data Protection Act 2018.

62 Section 3(1) of the Investigatory Powers Act 2016.

63 GIR Live Women in Investigations Conference on 12 June 2019. Report available at https://globalinvestigationsreview.com/article/1193967/osofsky-sfo-can-and-will-offer-immunity-deals.

64 See https://www.sra.org.uk/solicitors/guidance/warning-notices/use-of-non-disclosure-agreements-ndas--warning-notice/, as updated on 25 November 2019.

the SRA Handbook) should not be taken to prohibit the use of NDAs. However, it states that legal professionals (and those responsible for managing complaints within law firms) should ensure that they do not:

- use NDAs in circumstances in which the subject of the NDA may, as a result of its use, feel unable to notify the SRA or other regulators or law enforcement agencies of conduct that might otherwise be reportable;
- fail to notify the SRA of misconduct, or a serious breach of regulatory requirements, by any person or firm, including wrongdoing by the firm or harassment or other misconduct towards others such as employees or clients; or
- use NDAs as a means of improperly threatening litigation or other adverse consequences, or otherwise exerting inappropriate influence over people not to make disclosures which are protected by statute, or reportable to regulators or law enforcement agencies.

Inappropriate use of NDAs may constitute a breach of the SRA's Standards and Regulations (replacing the SRA Handbook) and lead to disciplinary action. The SRA's warning notice of March 2018 was echoed in the Law Society's practice note on 'Non-disclosure agreements and confidentiality clauses in an employment law context' published in January 2019.[65] This reiterates that NDAs cannot be used to prevent protected disclosures from being made to relevant bodies. It notes that whistleblowing in the public interest is a complex matter and that parties who wish to blow the whistle will often need professional help.

Practical questions 19.4.4

To whom to blow the whistle 19.4.4.1

An individual will need to give careful consideration to a decision to blow the whistle externally because this may result in the loss of statutory protection. To be a protected disclosure, the whistleblower must make a qualifying disclosure to an appropriate person or organisation.

In most cases, disclosures should be made to the employer. However, in some circumstances individuals may be protected if they disclose information externally.

Parliament has approved a list of 'prescribed persons' to whom a worker or an employee can make a disclosure, provided they believe the information is substantially true and concerns a matter within that person's area of responsibility. They include (but are not limited to) the SFO, the NCA, HMRC, the Health and Safety Executive and the CMA. There is no requirement to alert the employer beforehand.

Where the worker or employee reasonably believes a third party (such as a client or supplier) is responsible for the wrongdoing, they can report it to that third party without telling the employer.

65 See https://www.lawsociety.org.uk/support-services/advice/practice-notes/non-disclosure-agreements-and-confidentiality-clauses/.

Disclosure to other external sources (e.g. the media) is protected only if the individual believes that the information is substantially true and they do not act for gain. So, an individual who receives payment for a story to a newspaper will not be protected. Unless the matter is 'exceptionally serious', they must have already disclosed it to the employer or a prescribed person (or believe that, if they did, evidence would be destroyed or they would suffer reprisals). Disclosure to that person must also be reasonable.

19.4.4.2 Requests to sign an NDA

Any request to sign an NDA purporting to prevent an individual from raising whistleblowing concerns should be resisted and will be unenforceable.

See Section 19.2.3

19.4.4.3 Challenges to unfair treatment of whistleblowers

An individual who is a worker or employee and who is subjected to unfair treatment by their employing or engaging entity or by other employees or co-workers may have a claim in the employment tribunal against individuals and the entity.

See Section 19.2

20

Whistleblowers: The US Perspective

Daniel Silver and Benjamin A Berringer[1]

Overview of US whistleblower statutes 20.1

The US legal system contains a multitude of state and federal laws that protect individuals who report potential misconduct (whistleblowers) from retaliation for making the report.[2] Some of these laws protect specific classes of individuals, such as truck drivers,[3] nuclear engineers,[4] pilots[5] and miners.[6] Others relate to specific

1 Daniel Silver is a partner and Benjamin A Berringer is an associate at Clifford Chance US LLP.

2 The exact nature of this protection depends significantly on the statute that creates the protection. For example, the Surface Transportation Assistance Act states that 'no person' is allowed to 'discriminate' against truck drivers and certain other employees 'with respect to his compensation, terms, conditions, or privileges of employment' for making a whistleblower report. 49 U.S.C. § 31105. On the other hand, the Sarbanes-Oxley Act prohibits a broader range of conduct, but applies to a narrower class of employers. See infra notes 17 to 24 and accompanying text.

3 The Surface Transportation Assistance Act protects truck drivers and certain other employees from retaliation for reporting violations of regulations related to the safety of commercial vehicles. 49 U.S.C. § 31105.

4 The Energy Reorganization Act protects employees of operators, contractors and subcontractors of nuclear power plants licensed by the Nuclear Regulatory Commission from retaliation for reporting violations of the Atomic Energy Act of 1954. 42 U.S.C. § 5851.

5 The Federal Airline Deregulation Act's Whistleblower Protection Program protects employees, contractors, and subcontractors of air carriers from retaliation for, *inter alia*, reporting violations of laws related to aviation safety. 49 U.S.C. § 42121.

6 The Federal Mine Safety and Health Act of 1977 prohibits employment discrimination against a miner, representative of miners, or applicant for employment in any coal or other mine as a reprisal for making safety-related complaints. 30 U.S.C. § 815.

conduct such as motor vehicle safety issues,[7] violations of the Clean Air Act,[8] violations of the Clean Water Act[9] or violations of the Affordable Care Act.[10] Each of these laws is structured differently. As a result, the precise steps that a whistleblower must take to file a report, whether the whistleblower has a private right of action and the scope of protection may vary depending on the statutory basis for the whistleblower claim.[11]

20.1.1 The SEC whistleblower regimes

US securities laws protect whistleblowers who report potential misconduct by entities and individuals subject to regulation by the US Securities and Exchange Commission (SEC). This protection was originally created by the Sarbanes-Oxley Act (SOX) in 2002. It was then strengthened and expanded by the Dodd-Frank Act (DFA) in 2009, which created the Whistleblower Protection Program (the Program), pursuant to which individuals who voluntarily report 'original information'[12] about potential violations of federal securities laws are protected from retaliation and entitled to a financial award if the information leads to a successful judicial or administrative enforcement action in which the SEC obtains monetary sanctions over US$1 million.[13] The Program has been a significant success for the SEC. Since August 2011, the Program has received over 33,300 whistleblower reports from individuals in all 50 US states and 123 foreign countries.[14]

7 The Moving Ahead for Progress in the 21st Century Act prohibits discrimination by motor vehicle manufacturers, parts suppliers or dealerships against employees who provide information about any motor vehicle defect or violation of the Motor Vehicle Safety Act. 49 U.S.C. § 30171.

8 The Clean Air Act contains a provision protecting employees from retaliation for reporting violations of the Clean Air Act. 42 U.S.C. § 7622.

9 The Water Pollution Control Act contains a provision protecting employees from retaliation for reporting violations of the Act. 33 U.S.C. § 1367.

10 The Affordable Care Act protects employees from retaliation for reporting violations of certain of its provisions, including, *inter alia*, discrimination based on an individual's receipt of health insurance subsidies, denial of coverage for a pre-existing condition, and an insurer's failure to rebate a portion of an excess premium to customers. 29 U.S.C. § 218c.

11 Compare, e.g., 42 U.S.C. § 7622 (no private cause of action for whistleblower retaliation under the Clean Air Act), with 29 U.S.C. § 1132(a) (creating a private cause of action for the enforcement of ERISA provisions, including anti-retaliation provisions).

12 The US Securities and Exchange Commission (SEC) has defined original information as 'information derived from your independent knowledge (facts known to you that are not derived from publicly available sources) or independent analysis (evaluation of information that may be publicly available but which reveals information that is not generally known) that is not already known by us.' SEC, Office of the Whistleblower, Frequently Asked Questions, https://www.sec.gov/about/offices/owb/owb-faq.shtml. The SEC has also stated that information from certain individuals, including attorneys and fiduciaries, may not be deemed original. See infra notes 73 to 75 and accompanying text.

13 See 15 U.S.C. § 78u-6. Dodd-Frank also imposed a similar regime under the Commodity Exchange Act. See 7 U.S.C. § 26.

14 SEC, 2019 Annual Report to Congress – Whistleblower Program, 22 to 25 (2018), https://www.sec.gov/files/sec-2019-annual-report-whistleblower-program.pdf [2019 Annual Report on Whistleblower Program].

In fiscal year 2018 alone, the SEC received over 5,200 whistleblower reports, including 479 (9.5 per cent) from foreign whistleblowers.[15] As a result of these reports, the SEC has instituted enforcement actions that have resulted in penalties of more than US$2 billion and awarded over US$387 million to 67 different whistleblowers.[16]

The Program rewards individuals for making reports pursuant to both SOX and the DFA whistleblower provisions. Under both statutes, individuals qualify as whistleblowers if they report alleged misconduct and have 'a reasonable belief that the information [they are] providing relates to a possible securities law violation . . . that has occurred, is ongoing, or is about to occur'.[17] A belief is reasonable if it is both subjectively and objectively reasonable; that is, the employee must have both 'a subjectively genuine belief that the information demonstrates a possible violation, and that this belief is one that a similarly situated employee might reasonably possess'.[18]

To satisfy the subjective component of this standard, the employee must have 'actually believed the conduct complained of constituted a violation of pertinent law'.[19] For the objective component, '[the] employee need not show that an actual violation occurred so long as "the employee reasonably believes that the violation

15 Id. at 22, 33. A significant number of the international reports came from Germany (44 reports), the United Kingdom (44 reports) and Canada (71 reports).

16 Id. at 1.

17 17 C.F.R. § 240.21F-2(b)(i). Prior to 2011, the Department of Labor applied a 'definitively and specifically' standard to claims under the Sarbanes-Oxley Act (SOX), which required that the whistleblower show that the conduct was definitively and specifically related to one or more of the laws listed in SOX. See, e.g, *Welch v. Cardinal Bankshares Corporation*, ARB No. 05-064, ALJ No. 2003-SOX-15 (ARB 31 May 2007) (Whistleblower report related to deviation from generally accepted accounting practices was not necessarily protected activity under SOX because an accounting deviation is not inherently a violation of the securities laws). However, in a 2011 decision, the Department of Labor clarified that the reasonable belief standard applied. *Sylvester v. Parexel Int'l LLC*, ARB No. 07-123, ALJ Nos. 2007-SOX-039 to -042 (ARB 23 May 2011). The SEC has stated that a reasonable belief is sufficient under either statute. See Implementation of the Whistleblower Provisions of Section 21f of the Sec. Exch. Act of 1934, Release No. 64545 (S.E.C. Release No.), Release No. 34-64545, 101 S.E.C. Docket 630, 2011 WL 2045838, at *7, n. 36 (25 May 2011) [DFA Implementation Release] (adopting the reasonable belief standard and noting that the SOX anti-retaliation provision has the same requirement). However, at least some courts still apply the definitively and specifically standard for SOX claims. See, e.g., *Riddle v. First Tenn. Bank*, 497 F. App'x. 588 (6th Cir. 2012) ('[A]n employee's complaint must "definitively and specifically relate" to one of the six enumerated categories found in 18 U.S.C. § 1514A'). But see *Genberg v. Porter,* 882 F.3d 1249, 1255 (10th Cir. 2018) (holding that the 'definitive and specific' standard used by the District Court was 'obsolete' and reversing grant of summary judgment for defendant based on that standard); *Wiest v. Lynch*, 710 F.3d 121, 131 (3d Cir. 2013) (adopting reasonable belief standard based on *Sylvester* decision).

18 *Ott v. Fred Alger Mgmt., Inc.*, 2012 WL 4767200, at *4 (S.D.N.Y. 27 September 2012) (quoting DFA Implementation Release, at *7).

19 *Welch v. Chao*, 536 F.3d 269, 277 n.4 (4th Cir. 2008) (interpreting whether a plaintiff qualified for whistleblower status under SOX).

is likely to happen"'.[20] 'A belief is objectively reasonable when a reasonable person with the same training and experience as the employee would believe that the conduct implicated in the employee's communication could rise to the level of a violation of' the securities laws.[21]

While the standard for whistleblower status is similar under both statutes, there are also some material differences. First, there are differences in who is protected. SOX protects employees, contractors and subcontractors of publicly traded companies[22] and rating agencies from retaliation for reporting certain criminal offences (mail or wire fraud) or the potential violation of 'any rule or regulation of the Securities and Exchange Commission, or any provision of federal law relating to fraud against shareholders' either internally or to certain government entities.[23] The DFA, on the other hand, prohibits any employer from taking adverse employment actions against employees who report potential violations of the securities laws to the SEC.[24]

Second, there are differences in what misconduct can be reported. DFA protections only apply to whistleblowers who report potential violations of the securities laws, while SOX prohibits retaliation against whistleblowers who report potential violations of a wider range of laws.

Third, there are differences in the definition of retaliation. The DFA prohibits a broader range of retaliatory conduct. Pursuant to the statute, no employer 'may discharge, demote, suspend, threaten, harass, directly or indirectly, or in any other manner discriminate against, a whistleblower in the terms and conditions of employment because of any lawful act done by the whistleblower'.[25] The SOX prohibition is substantially similar, but it does not specifically prohibit indirect action against employees.[26]

Fourth, there are procedural differences in how whistleblowers must report the conduct. SOX specifically states that whistleblowers are protected against retaliation if they report misconduct internally to 'a person with supervisory authority

20 *Stewart v. Doral Fin. Corp.*, 997 F. Supp. 2d 129, 137 (S.D.N.Y. 2014) (quoting *Sylvester*, 2011 WL 2165854, at *13).

21 *Wiest*, 710 F.3d at 132.

22 The Supreme Court has ruled that this protection extends to employees of a non-public company who report fraud against shareholders of a public company that receives services from the non-public company. *Lawson v. FMR LLC*, 571 U.S. 429, 440 (2014).

23 18 U.S.C. § 1514A. Judicial decisions have made clear that disclosures regarding third parties are protected activity. See, e.g., *Sharkey v. J.P. Morgan Chase & Co.*, No. 10 Civ. 3824, 2011 WL 135026, at *5 to 6 (S.D.N.Y. 14 January 2011) (finding that the plaintiff properly pleaded that a report concerning a third-party client's illegal activity constituted a protected activity under SOX).

24 The Dodd-Frank Act (DFA) defines a whistleblower as 'any individual who provides . . . information relating to a violation of the securities laws to the Commission.' 15 U.S.C. § 78u-6(a)(6).

25 15 U.S.C. § 78u-6(h)(1)(A).

26 18 U.S.C. § 1514A(a) (identified classes of employers may not 'discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment because of any lawful act done by the employee').

over the employee (or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct)' or externally to a federal regulatory or law enforcement agency, or to the US Congress.[27] The DFA, on the other hand, statutorily defines a whistleblower as 'any individual who provides . . . information relating to a violation of the securities laws' to the SEC.[28] Recognising that SOX whistleblowers – who can report internally – are also protected under the DFA, the SEC attempted to extend DFA protection to whistleblowers who report internally pursuant to SOX.[29] This interpretation, however, was unanimously rejected by the Supreme Court, which held that the DFA only protects employees who report misconduct to the SEC.[30]

Finally, there are significant differences in how a whistleblower can bring a claim for retaliation. SOX is enforced by the Occupational Safety and Health Administration (OSHA), which is responsible for investigating claims.[31] Once a whistleblower makes a claim, OSHA will conduct an initial investigation to determine if the whistleblower has made a *prima facie* showing that their whistleblower report was a contributing factor to an unfavourable employment decision.[32] If OSHA comes to this determination, the employer can then rebut the claim with clear and convincing evidence.[33] Once OSHA makes a final finding, either party may appeal to the Department of Labor's Office of Administrative Law Judges (ALJ).[34] The regulations then allow for limited discovery, after which an ALJ will conduct a hearing and render a decision.[35] The ALJ's decision can be appealed by the unsuccessful party to the Department of Labor's Administrative Review Board,[36] with further appeal to the United States Circuit Court of Appeals for the circuit in which the employee resided or the violation allegedly occurred.[37] Additionally, a SOX whistleblower may bring a retaliation claim in federal court

27 18 U.S.C. § 1514A. Administrative decisions have made clear that disclosures to other entities, including the IRS and local law enforcement, may also be protected. See, e.g., *Vannoy v. Celanese Corp.,* ARB No. 09-118, ALJ No. 2008-SOX-064 (ARB 28 September 2011) (finding that disclosures to the IRS constituted protected activity under SOX); *Funke v. Federal Express Corp*., ARB No. 09-004, ALJ No. 2007-SOX-043 (ARB 8 July 2011) (finding that reports to local law enforcement constituted protected activity).

28 15 U.S.C. § 78u-6(a)(6). This provision arguably conflicts with the broader anti-retaliation provision of the DFA, which states that an employer cannot 'discharge, demote, suspend, threaten, harass, directly or indirectly, or in any other manner discriminate against, a whistleblower in the terms and conditions of employment' in retaliation for: (1) providing information to the SEC; (2) initiating, testifying in, or assisting an SEC investigation or action; or (3) making disclosures that are protected by the Sarbanes-Oxley Act or 'any other law, rule, or regulation subject to the jurisdiction of' the SEC. 15 U.S.C. § 78u-6(h)(1)(A).

29 17 C.F.R. § 240.21F-2.

30 *Digital Realty Tr., Inc. v. Somers*, 138 S. Ct. 767 (2018).

31 See 29 C.F.R. § 1980.104(e).

32 Id.

33 29 C.F.R. § 1980.104(e)(4).

34 29 C.F.R. § 1980.106.

35 29 C.F.R. §§ 1980.107, 1980.109.

36 29 C.F.R. § 1980.110.

37 29 C.F.R. § 1980.112.

if the Secretary of Labor 'has not issued a final decision within 180 days of the filing of [a] complaint and there is no showing that such delay is due to the bad faith of the claimant'.[38]

Individuals claiming DFA protections, on the other hand, may immediately bring a claim in federal court. There, courts will employ a burden-shifting standard. The employee must initially meet the 'rather light burden of showing by a preponderance of evidence that [the whistleblower report] tended to affect [the adverse action] in at least some way'.[39] Once the employee has made this *prima facie* showing of retaliation, the burden shifts to the employer to prove that there was a legitimate non-retaliatory reason for the decision.[40] Only if the employer is able to provide a non-retaliatory reason does the burden shift back to the employee to show that the proffered legitimate reason is a pretext.[41]

20.1.2 The CFTC whistleblower regime

The DFA added Section 23 of the Commodity Exchange Act (CEA), which provides for whistleblower protections. The CEA anti-retaliation provision is identical to the DFA provision in the Exchange Act. Although the CEA has been used less frequently than the SEC provision by employees, given the similarities between the two, the Commodity Futures Trading Commission (CFTC) began, among other things, to strengthen its anti-retaliation protections for whistleblowers and harmonise its rules with those of the SEC's Program in May 2017. The CFTC has also explicitly stated that it will rely on SEC precedent.[42]

20.2 The corporate perspective: preparation and response

20.2.1 Preparing for a whistleblower report

There is no legal requirement to create whistleblower policies, but companies that are potentially subject to SOX or DFA whistleblower requirements should ensure that they are prepared by creating policies and procedures that address how they will respond to and protect whistleblowers. These policies and procedures must be appropriately tailored to take into account factors such as the size of the company, the statutory whistleblower provisions that apply, and the nature of its business. At a minimum, whistleblower policies should include the following three types of guidance.

38 18 U.S.C. § 1514A(b)(1)(B).

39 *Feldman v. Law Enf't Assocs. Corp.*, 752 F.3d 339, 348 (4th Cir. 2014).

40 Implementation Release at 18, n. 41.

41 Id.

42 See In the Matter of Claims for Award by: Redacted WB-APP Redacted; and Redacted WB-APP Redacted, in Connection with Notice of Covered Action Redacted (1 January 2018) (The CFTC adopted principles 'consistent with those of the SEC's whistleblower program' to evaluate a whistleblower's award claim.). See also 17 C.F.R. §§ 165.15(A)(2), 165.7(F)–(1) (2017). (The CFTC replaced the Whistleblower Award Determination Panel with the Claims Review Staff (CRS). The CFTC stated that the CRS would include an enhanced review process 'similar to that established under the whistleblower rules of the US Securities and Exchange Commission.)

First, the whistleblower policy needs to make clear how an employee or external party can report information about potential misconduct. There are a number of methods that firms can use to facilitate whistleblower reports, including designating an employee from legal or compliance who will receive those reports, creating a web-based interface for making reports, or creating a telephone hotline. Ultimately, the company should adopt one or more methods that will best facilitate reports. Regardless of the method chosen, whistleblowers must also be able to escalate the report to a designated senior employee or board member in the event that the conduct implicates legal, compliance or senior executive management.

Second, the policy should explain how the company will investigate a whistleblower claim. This aspect of the policy should not mandate that specific steps will be followed in each case, as the actual nature and scope of any investigation will depend heavily on the nature and circumstances of the claim. Among the aspects that may be included are: (1) who is responsible for initially investigating a whistleblower claim; (2) who is responsible for making an initial determination on the merit of the claim; (3) the circumstances under which the company will conduct a more extensive investigation; and (4) who is responsible for ultimately evaluating the whistleblower report and implementing remedial improvements if necessary.

Finally, the policy should ensure that when the identity of a whistleblower is known and the whistleblower is an employee, steps are taken to protect that person from retaliation. This protection could include designating an employee from legal or compliance to monitor the status of the whistleblower to ensure that they are not subject to adverse actions. Additionally, the policy should make clear that any personnel who retaliate against a whistleblower will be subject to discipline.

Responding to a whistleblower report 20.2.2

Once a company learns that a whistleblower report has been made, it should adhere to its whistleblower policy. First, the company should assess the whistleblower's claim to determine what responsive action is appropriate. As discussed above, the nature of the inquiry will depend on the claim, but could range from an informal assessment by the compliance team to a formal investigation conducted by external counsel. Ultimately, the determination of how to investigate the claim will depend on the severity of the alleged conduct and the credibility of the claim. In conducting the inquiry, it is critical that the company make clear to any employees who are interviewed that even though the substance of the interview may be protected by the company's attorney–client privilege, the employee retains the right to disclose the facts discussed during the interview to the appropriate authorities.[43]

43 See, e.g., *In re KBR, Inc.*, Securities Exchange Act Release No. 74619 (1 April 2015) (KBR agreed to settle charges that its standard form confidentiality provision, which stated that witnesses needed permission of the company to disclose matters discussed in internal investigation interviews, undermined the Program.). The company should also ensure that similar language is used in any interview conducted by counsel as part of an internal investigation.

Second, in the case of a whistleblower report by an employee whose identity is known, in addition to the steps outlined in the whistleblower policy to protect the employee, the company should also ensure that it has documented any previous warnings or disciplinary actions taken against the employee, as well as adhere to consistent disciplinary procedures. Such documentation and adherence will, if necessary, support the company's position that a whistleblower employee was disciplined or terminated for conduct unrelated to a whistleblower report.

20.2.3 Defending anti-retaliation suits

If a whistleblower brings a retaliation action it will be difficult, if not impossible, to defeat the action at an early stage in the litigation. This difficultly exists because the standard for what constitutes an adverse employment action is purposely vague to allow for 'a factual determination on a case-by-case basis',[44] which has been interpreted by courts to reflect a 'congressional intent to prohibit a very broad spectrum of adverse action against . . . whistleblowers'.[45] As a result, courts have refused to create a bright-line standard for what constitutes an adverse employment action and instead 'pore over each case to determine whether the challenged employment action' constitutes an adverse action.[46] While any action can be construed by an employee as retaliatory, in practice, whistleblower claims are generally predicated on conduct, such as dismissals,[47] demotions[48] or decreased compensation.[49]

Despite these difficulties, there are certain defences that may be successfully asserted in a retaliation lawsuit. First, an employer can argue that there was no causal connection between the protected activity and the adverse employment decision.[50] Two factors that can sever the causal connection are the passage of time or a legitimate intervening event. The passage of time between a whistleblower's report and their termination can demonstrate that the adverse action was not retaliatory. The Second Circuit has declined to establish a bright-line rule,[51]

44 DFA Implementation Release, at *8.

45 *Anthony Menendez v. Halliburton, Inc.*, 2011 WL 4915750, at *10 (ARB 13 September 2011) (SOX anti-retaliation claim).

46 *Wanamaker v. Columbian Rope Co.*, 108 F.3d 462, 466 (2d Cir. 1997) (ADEA anti-retaliation claim).

47 See e.g., *Ott*, 2012 WL 4767200 at *3 (employee alleged that she was terminated for reporting to the SEC that she believed that the hedge fund's trading policy allowed the firm to trade ahead of customer orders).

48 See, e.g., *In re Paradigm Capital Management, Inc.*, S.E.C. File No. 3-15930 (2014) (hedge fund settled claims by SEC that it retaliated against an employee who was relieved of his responsibilities following complaint).

49 See, e.g., *O'Mahony v. Accenture Ltd.*, 537 F. Supp. 2d 506, 508 (S.D.N.Y. 2008) (SOX whistleblower allegations were adequately pled where defendant reduced plaintiff's level of responsibility and compensation shortly after plaintiff reported defendant's alleged fraudulent activity).

50 *Fraser v. Fiduciary Trust Co. Int'l*, No. 04 CIV. 6958 (PAC), 2009 WL 2601389, at *6 (S.D.N.Y. 25 August 2009) aff'd, 396 F. App'x 734 (2d Cir. 2010).

51 *Gorman–Bakos v. Cornell Coop. Extension*, 252 F.3d 545, 554 (2d Cir. 2001).

but in the absence of additional evidence of a defendant's retaliatory motive, the passage of two months may be sufficient to sever the causal connection.[52] However, to the extent that there is evidence of other retaliatory actions against the whistleblower, courts will allow for a longer gap between the protected activity and termination.[53] Similarly, a legitimate intervening event that occurs after the whistleblower's disclosure to the SEC will sever the causal connection and create a non-retaliatory justification for the termination. For example, one court granted summary judgment for an employer because, after making his disclosure to the SEC, the whistleblower told investors that the external directors were 'worthless', which provided a non-retaliatory justification for the whistleblower's dismissal.[54] However, because causation is generally a question of fact, a court is unlikely to decide as a matter of law that either the passage of time or an intervening event has severed the causal chain.[55]

An employer could argue that the whistleblower did not have a reasonable belief that the alleged conduct constituted a violation or potential violation of the securities law. In particular, whistleblower complaints need to provide more than 'self-serving averments'[56] or 'bald statement[s]'[57] in support of the claim that the plaintiff had a reasonable belief that the conduct was illegal.

There are certain defences that may be more applicable to either DFA or SOX whistleblower claims. First, DFA whistleblower claims may be amenable to arbitration. As a general principle, US federal courts 'strongly [favour] arbitration as an alternative dispute resolution process',[58] and statutory claims may be submitted to arbitration unless the statute explicitly prohibits arbitration.[59] As a result, some courts have held that DFA retaliation claims are amenable to arbitration, although a prohibition on arbitration was added to other whistleblower retaliation statutes by the DFA.[60] The Third Circuit, the only circuit court to examine this issue

52 *Garrett v. Garden City Hotel, Inc.*, No. 05-CV-0962, 2007 WL 1174891, at *21 (E.D.N.Y. 19 April 2007) (collecting cases).

53 See, e.g., *Mahony v. KeySpan Corp.*, No. 04 CV 554 SJ, 2007 WL 805813, at *6 (E.D.N.Y. 12 March 2007) (denying motion for summary judgment in SOX whistleblower case despite 13-month gap between protected activity and termination because a 'reasonable juror could find that the string of retaliatory acts culminating in Plaintiff's termination is evidence that Plaintiff's protected activity was a contributing factor in the adverse employment action').

54 *Feldman*, 752 F.3d at 349.

55 See, e.g., *Mahony*, 2007 WL 805813, at *6. ('The gap in time between protected activity and adverse employment action is merely one factor which a jury can consider when determining causation. A jury may look to other facts to decide whether the protected activity precipitated the adverse employment action, including evidence of a strained relationship between the parties that portended the employee's termination.')

56 *Livingston v. Wyeth Inc.,* 2006 WL 2129794, *10 (M.D.N.C. 28 July 2006).

57 *Nielsen v. AECOM Tech. Corp.*, 762 F.3d 214, 223 (2d Cir. 2014).

58 *Nat'l City Golf Fin. v. Higher Ground Country Club Mgmt. Co., LLC*, 641 F. Supp. 2d 196, 201 (S.D.N.Y. 2009).

59 *Shearson/Am. Express v. McMahon*, 482 U.S. 220, 226 (1987).

60 See, e.g., *Murray v. UBS Sec.*, LLC, 2014 WL 285093, *11 (S.D.N.Y. 27 January 2014) (holding SOX's prohibition on predispute arbitration does not apply to DFA retaliation claims); *Ruhe v.*

so far, has concluded that 'although Congress conferred on whistleblowers the right to resist the arbitration of certain types of retaliation claims, that right does not extend to Dodd-Frank claims arising under [the Dodd-Frank whistleblower provision]'.[61] SOX claims, on the other hand, are not arbitrable as a result of an amendment to SOX that was passed as part of the DFA.[62]

Finally, in some instances, an employer can argue that an anti-retaliation claim is barred because it is extraterritorial. In *Liu Meng-Lin v. Siemens AG*, for example, the Second Circuit held that DFA whistleblower protection does not generally apply extraterritorially and that the plaintiff, a resident of Taiwan who was employed by the Chinese subsidiary of a German company, did not have a valid anti-retaliation complaint because neither his report to superiors in China and Germany regarding allegedly corrupt activities that took place outside the United States, nor the decision by Siemens in Germany or China to terminate him, had a sufficient connection to the United States to treat it as a domestic application of the statute.[63] The Second Circuit, however, declined to 'define the precise boundary between extraterritorial and domestic applications' of the anti-retaliation provision because the case was 'extraterritorial by any reasonable definition'.[64] Nonetheless, this suggests that many foreign whistleblowers may not be protected by the DFA.[65]

20.2.4 Anti-retaliation suits by the SEC

In addition to potential suits by a whistleblower, the SEC has asserted an independent right to bring whistleblower retaliation claims. In June 2014, the SEC brought its first enforcement action against a registered investment adviser for retaliation.[66] Subsequent actions show that this remains an enforcement priority for the SEC.[67] In particular, the SEC may enforce the DFA anti-retaliation provision for 'conduct occurring outside the United States that has a foreseeable

Masimo Corp., 2011 WL 4442790, *5 (C.D. Cal. 16 September 2011) (refusing to read an anti-arbitration provision into 15 U.S.C. § 78u).

61 *Khazin v. TD Ameritrade Holding Corp*., 773 F.3d 488, 493 (3d Cir. 2014).

62 18 U.S.C. § 1514A(e)(2).

63 *Liu Meng-Lin v. Siemens AG*, 763 F.3d 175, 179-180 (2d Cir. 2014).

64 Id.

65 Employers may also be able to argue that the SOX whistleblower provisions do not apply to foreign employees. See, e.g., *Asadi v. G.E. Energy (USA) LLC*, No. 4:12-345, 2012 WL 2522599 (S.D. Tex. 28 June 2012) (Neither SOX nor DFA anti-retaliation provisions protected US citizen employed by US company who was temporarily relocated to a foreign country because 'the majority of events giving rise to the suit occurred in a foreign country'). But see *Walters v. Deutsche Bank, et al.*, 2008-SOX-70, slip op. at 41 (ALJ 20 March 2009) (US citizen working in Switzerland was protected as a whistleblower because 'all elements essential to establishing a *prima facie* violation of Section 806 allegedly occurred in the United States').

66 *In re Paradigm Capital Management, Inc*., S.E.C. File No. 3-15930 (2014).

67 See, e.g., *In re KBR, Inc*., S.E.C. File No. 3-16466 (2015) (cease and desist order forbidding KBR, Inc. from violating Rule 21F-17, which prohibits companies from taking any action to impede whistleblowers from reporting possible securities violations to the SEC and imposing civil monetary penalties of US$130,000 for violations).

substantial effect within the United States'.[68] Therefore, even if a company can successfully avoid a retaliation suit by a whistleblower on extraterritorial grounds, the SEC could still bring a suit for the same conduct.

The whistleblower's perspective: representing whistleblowers 20.3

In determining whether to advise a client to make a whistleblower report, there are several key preliminary considerations. First, if the client is implicated in the wrongdoing this will impact whether they receive a whistleblower award and the amount of any award. The SEC in the DFA Implementation Release noted that 'culpable whistleblowers can enhance the Commission's ability to detect violations of the federal securities laws, increase the effectiveness and efficiency of the Commission's investigations and provide important evidence for the Commission's enforcement actions'.[69] As such, pursuant to SEC regulations, the SEC 'will assess the culpability or involvement of the whistleblower in matters associated with the Commission's action or related actions' in determining the amount of a whistleblower award.[70] In at least one case, it appears that the SEC gave an award to a culpable whistleblower. In an April 2016 order, the SEC stated that a whistleblower was subject to a parallel proceeding and that the award was 'subject to an offset for any monetary obligations', including disgorgement, prejudgment interest, and penalty amounts that the whistleblower had yet to pay towards a judgment.[71] In ordering this relief, the SEC noted that the whistleblower had previously been advised of the potential offset and did not object.[72]

Second, counsel should consider whether the putative whistleblower is subject to any professional confidentiality obligations that would be implicated. In particular, SEC regulations generally exclude attorneys from recovering under the Program. Information obtained through communications that are subject to the attorney–client privilege or information obtained 'in connection with the legal representation of a client' is generally not considered 'original information'.[73] These exclusions are clearly directed at attorneys to 'send a clear, important signal to attorneys, clients, and others that there will be no prospect of financial benefit for submitting information in violation of an attorney's ethical obligations'.[74] Similarly, certain fiduciaries and professionals engaged by the company

68 15 U.S.C. § 78aa(b)(2).

69 DFA Implementation Release, at *89.

70 17 C.F.R. § 240.21F-6(b)(1).

71 Order Determining Whistleblower Award Claim, Exchange Act Release No. 34-77530, 2016 WL 1328926 (5 April 2016).

72 Id.

73 See 17 C.F.R. § 240.21F-4(b)(4)(i)-(ii).

74 See DFA Implementation Release, at *27. The SEC has, however, provided for exceptions to the attorney exclusions in order to balance an attorney's ethical obligations with the desire to prevent securities law violations. As a result, information obtained through a confidential communication or legal representation will be deemed 'original information' in three situations: (1) if the attorney is representing an issuer and reasonably believes that the disclosure is necessary to prevent the issuer from committing a material violation of the securities law or to rectify a material violation,

who obtained the information through those roles are generally not deemed to have 'original information' about misconduct.[75] However, there is no general bar on the use of information that is otherwise deemed confidential by a company.

20.3.1 Disclosing to the SEC

Neither DFA nor SOX whistleblower provisions mandate that a whistleblower make their initial disclosure to the SEC. Therefore, a whistleblower can choose to disclose initially to the SEC or first make an internal report to the employer.

From a rewards perspective, there is no benefit to disclosing first to the SEC. Pursuant to SEC regulations, the date of a whistleblower's initial internal report will be treated as the date of disclosure to the SEC, so long as the whistleblower makes a report to the SEC within 120 days of the internal report or a report to another federal agency.[76] Therefore, delaying SEC disclosure to make an internal report first will not affect whether the whistleblower is the first person to provide original information and thereby qualifies for an award.[77]

Moreover, reporting directly to the SEC could, in theory, reduce an award as one of the factors that the SEC considers in determining the amount of an award is whether the whistleblower reported the potential misconduct through internal company compliance systems and whether the whistleblower co-operated with any internal investigations.[78] Therefore, reporting directly to the SEC could reduce an award if the whistleblower is perceived to have circumvented the company's internal reporting system.

However, there is one major potential benefit to first disclosing to the SEC – guaranteed protection as a whistleblower under the DFA. In particular, the Supreme Court has held that individuals must report to the SEC in order to

---

which is likely to cause substantial injury to financial interests, or to prevent perjury or fraud upon the SEC in the course of an SEC investigation or administrative proceeding; (2) when allowed to make the disclosure pursuant to applicable state attorney conduct rules; or (3) 'otherwise'. The SEC has not provided guidance on the circumstances that would qualify an attorney to invoke the 'otherwise' exclusion.

75 17 C.F.R. § 240.21F-4(b)(4)(iii). The SEC has stated that information from these sources will not be deemed 'original' if: (1) the whistleblower is in a leadership position and learned the information either from another person or in connection with internal compliance procedures; (2) the whistleblower is an internal audit or compliance employee or external adviser; (3) the whistleblower was retained to conduct an internal investigation into the company; or (4) the whistleblower is an employee of a public accounting firm, and the information was obtained while performing a function required under the federal securities laws, and relates to a violation by the client or its employees.

76 17 C.F.R. § 240.21F-4(b)(7); see also, In re the Claim for an Award in Connection with [Redacted], Securities Exchange Act of 1934 Release No. 82996 (5 April 2018) (awarding US$2.2 million to whistleblower who initially provided notification to another federal agency).

77 See 17 C.F.R. § 240.21F-4(b) (defining 'original information' as information '[n]ot already known to the Commission for any other source').

78 See 17 C.F.R. § 240.21F-6(a)(4).

be protected as whistleblowers under the DFA.[79] Therefore, if an employee only makes an internal report, the employee will lose the anti-retaliation protection provided by the DFA.[80] Moreover, because the SEC treats all whistleblower complaints as confidential and the Program provides additional confidentiality protections to ensure that a whistleblower's identity is protected, whistleblowers receive an added protection through SEC disclosure.[81]

Once a whistleblower decides to make a report to the SEC, the process itself is fairly simple. Whistleblowers may submit a complaint either through the online Tips, Complaints, and Referrals (TCR) Portal on the SEC's whistleblower website or by mailing or faxing a TCR Form to the SEC Office of the Whistleblower.[82] Once the form is received, it will be reviewed by Division of Enforcement staff, who will then determine who is best placed to investigate the allegations.[83] In some instances, the TCR will be sent to another federal or state enforcement agency, in which case information that could identify the whistleblower is generally withheld.[84]

Recent SEC and CFTC awards 20.3.2

The SEC awarded over US$168 million in whistleblower awards to 13 individuals in fiscal year 2018, including the largest awards to date.[85] On 19 March 2018, the SEC awarded US$83 million to three whistleblowers related to the SEC's US$415 million settlement with Merrill Lynch in 2016, with two whistleblowers sharing approximately US$50 million and the third receiving US$33 million for their significant information, prompting the SEC to open two investigations and their ongoing assistance.[86] On 6 September 2018, the SEC awarded US$39 million to one whistleblower, the second-largest award in history of the Program, and US$15 million to another for their critical information and continued assistance

79 *Digital Realty*, 138 S. Ct. at 769; see also *Verble v. Morgan Stanley Smith Barney, LLC*, No. 3:14-CV-74, 2015 WL 8328561 (E.D. Tenn. 8 December 2015) (employee who was dismissed for assisting federal authorities, including the FBI, was not a protected whistleblower because he had not provided information to the SEC).

80 *Digital Realty*, 137 S.Ct. at 769.

81 17 C.F.R. § 240.21F-7. For added protection, a whistleblower may also submit a complaint anonymously through an attorney. See 2015 Annual Report at 17.

82 See https://www.sec.gov/about/offices/owb/owb-tips.shtml.

83 See SEC, Division of Enforcement, Enforcement Manual (4 June 2015), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

84 Id.

85 2019 Annual Report on Whistleblower Program, supra note 14, at 1.

86 SEC, press release, 'SEC Announces Its Largest-Ever Whistleblower Awards', https://www.sec.gov/news/press-release/2018-44; see also Pete Schroeder, 'U.S. SEC Awards Merrill Lynch Whistleblowers a Record $83 Million', *Reuters*, 19 March 2018, https://www.reuters.com/article/us-usa-sec-whistleblower/u-s-sec-awards-merrill-lynch-whistleblowers-a-record-83-million-idUSKBN1GV2MT; 2019 Annual Report on Whistleblower Program, supra note 14, at 10.

related to an undisclosed investigation.[87] On 26 March 2019, the SEC awarded US$50 million to two whistleblowers related to the SEC's US$367 million settlement with JPMorgan Chase & Co in 2015, with one whistleblower receiving US$37 million – the third-largest award – and the other US$13 million for their information and assistance.[88]

In addition to the aforementioned trend, on 24 May 2019, the SEC granted its first award under the internal reporting provision of the Program.[89] According to the SEC, the whistleblower sent an anonymous tip-off of alleged wrongdoings to his company before submitting the same information to the SEC within 120 days. The company opened an internal investigation and reported the allegations of misconduct to the SEC, which then opened its own investigation. The company also reported the results of its internal investigation, leading the SEC to take enforcement actions. The SEC credited the whistleblower for the results of the company's internal investigation and awarded him over US$4.5 million.

The SEC has also granted whistleblower awards to individuals who have engaged in reported misconduct. On 14 September 2018, the SEC provided a financial award to a claimant, although the claimant 'unreasonably delayed in reporting information to the Commission and was culpable'.[90] Similarly, on 26 March 2019, the SEC awarded a whistleblower (Claimant A) an unreported sum, despite Claimant A's participation in the reported misconduct.[91]

The CFTC has also shown an upward trend in granting whistleblower awards in increasing amounts. Starting with its first award of US$246,000 on 20 May 2014, the CFTC issued one award for US$300,000 in 2015, two awards for a total of US$11,551,320 in 2016, five awards for a total of US$75,575,113 in 2018, and five awards for a total of approximately US$15 million in the 2019 fiscal year.[92] Similarly, the CFTC's whistleblower programme has seen significant advancement and growth.

The three most notable CFTC whistleblower awards took place in 2018. On 12 July 2018, the CFTC granted its largest award of approximately US$30 million to one whistleblower who provided key information related to the 2015 settlement

87 SEC, press release, 'SEC Awards More Than $54 Million to Two Whistleblowers', https://www.sec.gov/news/press-release/2018-179.

88 SEC, press release, 'SEC Awards $50 Million to Two Whistleblowers', https://www.sec.gov/news/press-release/2019-42; see also Matt Robinson and Neil Weinberg, 'Whistleblowers Awarded $50 Million by SEC in JPMorgan Case', *Bloomberg*, 26 March 2019, https://www.bloomberg.com/news/articles/2019-03-26/two-whistleblowers-awarded-50-million-for-aiding-sec-case.

89 SEC, press release, 'SEC Awards $4.5 Million to Whistleblower Whose Internal Reporting Led to Successful SEC Case and Related Action', https://www.sec.gov/news/press-release/2019-76.

90 SEC, Release No. 84125 (14 September 2018).

91 SEC, Release No. 85412 (26 March 2019). Claimant A's reward was reduced because Claimant A delayed reporting and continued to passively benefit financially from the 'underlying misconduct during a portion of the period of delay'.

92 US Commodity Futures Trading Commission (CFTC), Annual Report on the Whistleblower Program and Customer Education Initiatives (October 2019), https://whistleblower.gov/sites/whistleblower/files/2019-10/FY19%20Annual%20Whistleblower%20Report%20to%20Congress%20Final.pdf.

with JPMorgan Chase & Co, which also settled with the SEC.[93] On 16 July 2018, the CFTC gave an award to a foreign whistleblower for the first time, providing over US$70,000 for significant contributions to the CFTC investigation and demonstrating the international reach of the whistleblower programme through an online system.[94] On 2 August 2018, the CFTC granted multiple whistleblower awards of more than US$45 million in total, and the Director of the CFTC's Division of Enforcement announced he expected the trend to continue.[95]

Filing a qui tam action under the False Claims Act 20.4

Individuals who report fraud against the United States government have another option for disclosing information – the False Claims Act. This Act was created in 1863 initially to combat price-gouging during the Civil War, but the modern incarnation of the statute is a result of congressional concern regarding defence procurement fraud.[96] Since the statute was enhanced in 1986, there has been a significant growth in False Claims Act suits, from 30 in 1987 to 674 in 2017.[97] As a result of these suits, the US Department of Justice (DOJ) collected US$56 billion between 1986 and 2017, including US$3.4 billion in the 2017 fiscal year alone.[98]

The False Claims Act can be used to prosecute claims for false monetary claims against the government, false statements in aid of false claims, conspiracies to defraud the government into paying a false claim, or false statements intended to reduce an obligation to the government.[99] Moreover, pursuant to the False Claims Act, private individuals – referred to as relators – may bring *qui tam* claims on behalf of the government alleging that a defendant has committed fraud against the US government.[100] If the prosecution of the *qui tam* claim is successful, the

93 CFTC, press release, 'CFTC Announces Its Largest Ever Whistleblower Award of Approximately $30 Million', https://www.cftc.gov/PressRoom/PressReleases/7753-18; Henry Cutter, 'JPMorgan Whistleblower Set to Get Largest Payout from CFTC', *Wall St.* J., 12 July 2018, https://www.wsj.com/articles/jpmorgan-whistleblower-set-to-get-largest-payout-from-cftc-1531421603?mod=djemRiskCompliance&ns=prod/accounts-wsj.

94 CFTC, press release, 'CFTC Announces First Whistleblower Award to a Foreign Whistleblower', https://www.cftc.gov/PressRoom/PressReleases/7755-18.

95 CFTC, press release, 'CFTC Announces Multiple Whistleblower Awards Totaling More than $45 Million', https://www.cftc.gov/PressRoom/PressReleases/7767-18.

96 *United States ex rel. Springfield Terminal Ry. Co. v. Quinn*, 14 F.3d 645, 649-51 (D.C. Cir. 1994). Defence contracting remains one of the most frequent targets of *qui tam* complaints, constituting approximately 14 per cent of *qui tam* complaints. The healthcare industry is the most frequent target, accounting for approximately 58 per cent of *qui tam* complaints. US Dep't of Justice (DOJ), Fraud Statistics – Overview: 1 October 1987 – 30 September 2017 (19 December 2017), https://www.justice.gov/opa/press-release/file/1020126/download.

97 Id.

98 DOJ, press release, 'Justice Department Recovers Over $3.7 Billion From False Claims Act Cases in Fiscal Year 2017', (21 December 2017), https://www.justice.gov/opa/pr/justice-department-recovers-over-37-billion-false-claims-act-cases-fiscal-year-2017.

99 31 U.S.C. § 3729.

100 31 U.S.C. § 3730(b).

relator may receive between 15 per cent and 30 per cent of the recovery.[101] This can result in substantial compensation for a whistleblower, as False Claims Act defendants may be liable for penalties of US$5,000 to US$10,000 per violation and for treble damages.[102]

20.4.1 How a qui tam action operates

To bring a *qui tam* action, the relator must file their complaint in federal court under seal.[103] The initial complaint is only served on the DOJ, which has 60 days to examine the merits of the claim.[104] During this 60-day period (which is often subject to extensions), the DOJ will determine whether to terminate or settle the claim, intervene and take 'primary responsibility' for the claim, or decline to intervene and allow the relator to proceed alone.[105] After this period expires, the complaint is unsealed and the defendant will receive notice of the claim.

At this stage, the government's 'ultimate election among the options has a direct effect on the relator's right to share in a recovery'.[106] If the government decides to intervene in the action, the relator is entitled to 15 per cent to 25 per cent of any recovery, while the government receives the remaining recovery.[107] The precise amount will 'depend upon the extent to which the person substantially contributed to the prosecution of the action'.[108] If, on the other hand, the government decides not to pursue the case, the relator will be entitled to 25 per cent to 30 per cent of the recovery, with the government again receiving the remainder of the recovery. The relator is also entitled to 'an amount for reasonable expenses which the court finds to have been necessarily incurred, plus reasonable attorneys' fees and costs'.[109] However, one study has revealed that the majority of plaintiffs voluntarily dismiss the *qui tam* action if the DOJ declines to intervene,[110] despite the potential for a larger award.

In addition to this basic framework, there are also limitations on awards, which may reduce or eliminate a possible award. First, a relator's award will be reduced if they 'planned and initiated' the False Claims Act violation.[111] Second, if the court determines that the information is 'based primarily on disclosures of

101 See 31 U.S.C. § 3730(d). However, as discussed further below, this can in some circumstances be reduced to 10 per cent or less. See infra notes 112 to 114 and accompanying text.

102 31 U.S.C. § 3729.

103 31 U.S.C. § 3730(b).

104 31 U.S.C. § 3730(b).

105 31 U.S.C. § 3730(b)-(c).

106 *Roberts v. Accentur*e, LLP, 707 F.3d 1011, 1015 (8th Cir. 2013).

107 31 U.S.C. § 3730.

108 Id.

109 Id.

110 See David Freeman Engstrom, 'Public Regulation of Private Enforcement: Empirical Analysis of DOJ Oversight of Qui Tam Litigation Under the False Claims Act', 107 *Nw. U. L. Rev.* 1717, 1718 (stating that in a randomly selected 460 case subsample of the 4,000 unsealed *qui tam* actions filed between 1986 and 2011 'roughly 60% of cases in which DOJ declined intervention appeared to generate no further litigation prior to a voluntary dismissal by the relator').

111 31 U.S.C. § 3730(d)(3).

specific information' relating to governmental investigations or news accounts, the award will be reduced to no more 'than 10 percent of the proceeds, taking into account the significance of the information and the role of the person bringing the action in advancing the case to litigation'.[112] Finally, a relator is entitled to no award if they are 'convicted of criminal conduct arising from his or her role in the violation'.[113] Additionally, there are provisions that preclude filing additional suits based on substantially similar *qui tam* or government enforcement proceedings.[114] These provisions are intended to achieve 'the golden mean between adequate incentives for whistle-blowing insiders . . . and discouragement of opportunistic plaintiffs who have no significant information to contribute of their own'.[115]

In addition to determining the quantum of a *qui tam* award, the DOJ's decision may also have a substantial impact on the outcome of the lawsuit. Statistics published by the DOJ show that cases where the DOJ intervenes are substantially more likely to generate recoveries than declined cases.[116] DOJ declination may also signal a lack of merit to the court.[117]

Recently enacted DOJ policy also encourages DOJ attorneys to 'consider whether the government's interests are served' by seeking dismissal of the *qui tam* action.[118] Pursuant to this policy, DOJ attorneys are encouraged to seek dismissal in order to (1) curb meritless *qui tam* actions, (2) prevent 'parasitic or opportunistic' actions that duplicate a pre-existing investigation, (3) prevent interference with government programmes, (4) preserve the DOJ's litigation prerogatives, (5) safeguard national security, (6) preserve government resources or (7) address 'egregious procedural errors' that would frustrate a proper investigation.[119]

---

112 31 U.S.C. § 3730(d)(1).

113 Id.

114 31 U.S.C. § 3730(e)(4)(A).

115 *United States ex rel. Springfield Terminal R. Co. v. Quinn*, 14 F.3d 645, 649 (D.C. Cir. 1994).

116 See DOJ, Fraud Statistics – Overview: 1 October 1987 – 30 September 2015 (12 July 2016), https://www.justice.gov/civil/file/874921/download (indicating that settlements and judgments in qui tam actions where the government intervened represented 94 per cent of all *qui tam* settlements and judgments obtained between 1987 and 2015).

117 See, e.g., *United States ex rel. Jamison v. McKesson Corp.*, 649 F.3d 322, 331 (5th Cir. 2011) (noting that DOJ decision to intervene in cases involving 7 of 400 defendants suggested that the unintervened claims 'presumably lacked merit'); *United States ex rel. Karvelas v. Melrose-Wakefield Hosp.*, 360 F.3d 220, 242 n.31 (1st Cir. 2004) ('[T]he government's decision not to intervene in the action also suggested that [relator's] pleadings of fraud were potentially inadequate.'); *United States ex rel. Mikes v. Straus*, 78 F. Supp. 2d 223, 225-26 (S.D.N.Y. 1999) (suggesting that 'the reason the Government chose not to intervene in this matter is its recognition that Relator's allegations . . . were a 'stretch' under the False Claims Act'). But see *United States ex rel. Williams v. Bell Helicopter Textron Inc.*, 417 F.3d 450, 455 (5th Cir. 2005) (noting that 'a decision not to intervene may not [necessarily be] an admission by the United States that it has suffered no injury in fact, but rather [the result of] a cost-benefit analysis' (citations and internal quotation marks omitted)); *United States ex rel. Downy v. Corning*, Inc., 118 F. Supp. 2d 1160, 1170 (D.N.M. 2000) (noting that intervention decision may have been driven by a 'lack of available Assistant United States Attorneys' or 'respect for the skill of the relator's attorneys').

118 DOJ, Justice Manual § 4-400.

119 Id.

However, even if the DOJ decides not to intervene a case, it still has an oversight role in the litigation. First, the DOJ retains the continuing right to dismiss or settle an action being prosecuted by a relator,[120] although at least some courts have suggested that this is not an absolute right.[121] Second, the DOJ retains the right to veto private dismissals or settlements because any judgment will have preclusive effect on a future lawsuit by the US government based on the same facts.[122] That said, a minority of courts have held that the DOJ can only object by showing 'good cause' in a case where it has not intervened.[123]

20.4.2 Effects of filing a qui tam action

A *qui tam* action can have a substantial impact on both the relator and the defendant. First, the relator faces both reputational and financial risk. By filing a *qui tam* action the relator has agreed to be publicly identified because the unsealed complaint will identify them as the complainant.[124] Relators have tried to avoid this consequence by moving to dismiss and seal cases if the DOJ declines to intervene, but have met with, at best, limited success.[125] For relators who are still employed by the defendant, this risk is mitigated by the anti-retaliation provisions in the False Claims Act, which provide for reinstatement and double damages in the event of retaliation.[126] Nonetheless, depending on the situation, relators may have legitimate concerns about the impact on their professional reputations.

Relators often face additional financial risks if the government declines to intervene. In particular, relators may be responsible for the defendant's reasonable legal fees if the defendant prevails and 'the court finds that the claim of the person

120 31 U.S.C. § 3730(c)(2)(b).

121 See *United States ex rel. Sequoia Orange Co. v. Baird-Neece Packing Corp.*, 151 F.3d 1139, 1145 (9th Cir. 1998) ('A two step analysis applies here to test the justification for dismissal: (1) identification of a valid government purpose; and (2) a rational relation between dismissal and accomplishment of the purpose.') [Internal citations and quotations omitted.]

122 See, e.g., *Searcy v. Philips Elecs. N. Am. Corp.*, 117 F.3d 154, 160 (5th Cir. 1997) (noting the 'danger that a relator can boost the value of settlement by bargaining away claims on behalf of the United States').

123 *United States ex rel. Killingsworth v. Northrop Corp.*, 25 F.3d 715, 722 (9th Cir. 1994); but see *Ridenour v. Kaiser-Hill Co.*, 397 F.3d 925, 931 n.8 (10th Cir. 2005). ('Even where the Government has declined to intervene, relators are required to obtain government approval prior to entering a settlement or voluntarily dismissing the action.')

124 *United States ex rel. Wenzel v. Pfizer, Inc.*, 881 F. Supp. 2d 217, 222–23 (D. Mass. 2012) ('[Relator] filed his claim with the expectation that his identity would be revealed to the public in the event that the government entered the case'). Relators have attempted to avoid this outcome by filing under a pseudonym or creating a corporation to file the complaint. This strategy, however, will only work if the case is not litigated. If it is litigated, this is unlikely to provide significant protection because the defendant is likely to seek discovery regarding the relator's identity and the basis of their knowledge. Moreover, in some cases there is no way to effectively hide the source of the information. See, e.g., id. at 223 (noting that 'it is doubtful that redaction would provide any protection given the very specific allegations contained in the complaint').

125 Id. at 221 (collecting cases and noting that '[m]ost courts have . . . decided that a relator's general fear of retaliation is insufficient to rebut the presumption of public access').

126 31 U.S.C. § 3730(h).

bringing the action was clearly frivolous, clearly vexatious, or brought primarily for purposes of harassment'.[127]

A *qui tam* action also creates financial and reputational risks for a defendant. A successful *qui tam* action could cost a corporation millions, if not billions, of dollars.[128] Moreover, defendants also risk debarment from additional federal contracts.[129] From a reputational perspective, the corporation faces negative publicity associated with public accusations of committing fraud against the government, although at least one court has suggested that this impact is minimised when the DOJ declines to intervene.[130]

127 31 U.S.C. § 3730(d)(4). US courts also have the inherent authority to impose sanctions, as well as authority pursuant to Rule 11 of the Federal Rules of Civil Procedure.

128 See DOJ, press release, 'GlaxoSmithKline to Plead Guilty and Pay $3 Billion to Resolve Fraud Allegations and Failure to Report Safety Data' (2 July 2012), https://www.justice.gov/opa/pr/glaxosmithkline-plead-guilty-and-pay-3-billion-resolve-fraud-allegations-and-failure-report (announcing settlement of civil and criminal actions against pharmaceutical company, including a US$1.043 billion settlement resolving four related *qui tam* actions).

129 31 U.S.C. § 3729 (2012).

130 *United States ex rel. Pilon v. Martin Marietta Corp*., 60 F.3d 995, 999 (2d Cir. 1995). ('[A] defendant's reputation is protected to some degree when a meritless qui tam action is filed, because the public will know that the government had an opportunity to review the claims but elected not to pursue them.')

21

Whistleblowers: The In-house Perspective

Steve Young[1]

21.1 Initial considerations

Most whistleblowing policies provide several channels for staff to raise concerns. These often include the staff member's line manager (or a more senior manager), human resources, audit, legal, compliance or dedicated ethics, or integrity, departments.

The desired culture of any corporate must be that staff feel entirely comfortable raising concerns with their immediate line manager, who in turn will escalate the issue to the appropriate department. Should whistleblowers prefer not to go to their line manager, they should feel able to approach someone in the organisation they trust. The culture corporates should aspire to must be one where employees may raise concerns with the full confidence they will be treated with respect, will be taken seriously and will suffer no retaliation in any form.

From an in-house perspective, it is always an initial concern that an employee has not had sufficient confidence in the organisation to raise the concern via internal personnel in the normal course of business. Resorting to the whistleblowing channels sends a message itself, and more so if the employee has chosen to remain anonymous. Monitoring and analysing whistleblowing cases can provide a measure of the organisation's culture and confidence levels for raising concerns. While much depends on the nature of the concern, the tone from the top and creating a culture that speaking up is the right thing to do are imperative. Many organisations now include questions in employee opinion surveys to try to gauge the level of confidence staff have in raising their concerns. Some other initial considerations are pointed out below.

1 Steve Young is the CEO of the Association of Corporate Investigators and head of fraud and investigations at Banque Lombard Odier & Co Ltd.

Culture: Creating a culture in which staff have confidence to raise concerns internally is becoming increasingly important as some regulatory authorities now mandate regulated firms to include regulatory whistleblowing hotline numbers and email addresses in corporate whistleblowing policies, for example at UK branches of overseas banks.[2] Additionally, proposals to extend the scope of whistleblower awards, for example the US Securities and Exchange Commission's proposal to allow awards based on information from a whistleblower that leads to deferred prosecution agreements and non-prosecution agreements entered into by the US Department of Justice,[3] if adopted, raises the possibility of direct reporting to regulators bypassing internal reporting channels.

Anonymity: Anonymous whistleblowers can deny the investigator the opportunity to open a constructive dialogue to seek further information, put matters into context and limit feedback. A key challenge for the investigator is why the whistleblower wished to remain anonymous. It can be helpful to simply ask the question if there is a communication channel, such as webmail, open with the whistleblower.

The nature of the allegation and motive for reporting: While investigators should always keep an open mind, the motive of the whistleblower often becomes apparent as the facts are established. If a dialogue with the whistleblower exists, they can be asked their motive for reporting.

Duration: How long the alleged conduct has been taking place is material. Aged issues can present problems such as records retention periods. In addition, because of staff turnover, accessibility to ex-employees can be a problem.

Existing knowledge from another source: Investigators should check corporate records, such as audit, risk, legal and compliance, to check if the alleged activity is known and was previously or is currently the subject of investigation.

Need for external counsel: Investigators should lean towards caution during the initial review of a whistleblower allegation and take legal advice at an early stage. Assessment of the legal risks by an internal or external lawyer will prevent problems arising later if the investigation uncovers serious wrongdoing.

The welfare of the whistleblower and duty of care: Investigators should keep in mind the welfare of the whistleblower. For most it will not have been an easy decision to speak up. Stay mindful of health and performance impacts – and the legal risk of these to the organisation.

Protecting the whistleblower from retaliation: In the event that a whistleblower is identified, immediate steps may need to be considered to prevent retaliation. These could include moving the whistleblower to another part of the organisation, or transferring to an alternative line manager. Much depends on the nature of the case.

2 See https://www.fca.org.uk/publication/policy/ps17-07.pdf.

3 See https://www.sec.gov/news/press-release/2018-120.

21.2 Identifying legitimate whistleblower claims

Given the wide range of concerns raised by whistleblowers, distinguishing between legitimate and non-legitimate allegations should be dictated by the facts gathered during the the investigation. In some cases, a prompt review of the matters alleged by a subject-matter expert can quickly point to whether something is 'off-target' or requires further investigation. During the normal course of document examination, email reviews, staff interviews and data analysis generally the allegations can be substantiated or disproved. While some allegations will always be inconclusive, more frequently in human resources cases, generally a determination can be reached on the facts. Whistleblowing cases that contain multiple allegations require a detailed breakdown of each allegation as some parts may prove substantive while others will be off-target. Whistleblowing allegations are never suited to a one-size-fits-all approach and much depends on the nature of each case.

On receipt of a whistleblowing allegation, first steps should include checks to ascertain if the matters raised are known or the subject of an ongoing or previous investigation.

Generally, allegations can be split into three categories:

- Material allegations that expose the corporate to regulatory action, civil claims or criminal investigation. These require experienced legal advice and depending on the jurisdiction investigation by external counsel to preserve privilege and advise the corporate accordingly.
- Allegations of wrongdoing, including internal fraud and breaches of the code of conduct or policies and procedures. These generally can be investigated by internal corporate investigators, or external forensic firms with internal or external legal advice and oversight if required.
- Behavioural allegations such as bullying, harassment, inappropriate relationships, etc., which can generally be investigated by human resources or independent line management. Allegations of a sexual nature may require specialist investigative expertise. The nature of these allegations should be reviewed to consider who is best suited to undertake the investigation. The #MeToo movement has seen an increase in sexual allegations that may require specialist investigative, legal and victim care management.

21.3 Employee approaches to whistleblowers

A key component of any corporate whistleblowing policy must include a zero-tolerance approach to any retaliation against a whistleblower. Retaliation or perceived retaliation against a whistleblower raises cultural and legal risk, and undermines the effectiveness of a whistleblowing programme. Frequently during whistleblowing investigations, especially ones involving allegations of wrongdoing by senior management, interviewees speculate as to who the whistleblower might be. Ideally, in the absence of a legal obligation to do so (e.g., in litigation or in some jurisdictions) it is preferable that there is no such disclosure.

Speculation among staff should be discouraged, as it can increase the risk of retaliation.

Retaliation against whistleblowers can take many forms; examples include silence, isolation, inappropriate remarks, threats and work sabotage. In the event that a staff member or number of staff members are acting inappropriately towards a whistleblower, action will need to be taken.

Good investigation process separates the collection of facts and evidence gathering from decision-making to determine outcomes. This is particularly important when an investigator is putting forward information concerning retaliation against a whistleblower. As a general rule the investigator should not be involved in the sanctions or enforcement actions against retaliators – it is a separate legal and HR issue.

If the whistleblower's identity is known, dialogue should take place about the treatment the whistleblower is receiving and whether he or she has disclosed to anyone that they have raised the matter. Special care is required if the retaliation is by a line manager. The whistleblower should be given an opportunity to express his or her expectations and view as to what could be done. Investigators should be mindful that the organisation will generally have a duty of care and the whistleblower could take action against the organisation in the future.

Frequently whistleblowers experiencing retaliation or those believing they are being treated differently suffer health problems, such as stress leading to time off work. In these circumstances, referrals via human resources to confidential staff welfare support schemes should be considered. In determining the action to be taken against staff involved in retaliation against a whistleblower, the investigator should consult with human resources, legal, compliance and business management functions for the next steps, which could include disciplinary action up to and including dismissal.

Appropriate action taken against those who retaliate against whistleblowers can send a strong message to reinforce the culture of the organisation.

Distinctive aspects of investigations involving whistleblowers 21.4

Corporates with in-house investigation departments generally have investigation procedures in place that also apply to whistleblowing cases. The substantive difference is how the matter was raised. Investigators should proceed with the protection of the whistleblower as a top priority. Thought should be given to lines of enquiry or staff interviews that could identify the whistleblower. The general rule to note is that it is the matter under investigation that is the issue, not how the matter came to the organisation's attention.

Investigators should check if local law requires disclosure that the matter was raised as the result of a whistleblower. It is generally not a requirement in law to disclose to those facing allegations that the matter under investigation was raised by a whistleblower.

A good example of an exception is France, where it is generally required that accused persons be informed of whistleblowing allegations made against them so they may respond to them. They also have protection against malicious allegations. In this respect investigators should be mindful that, in the rare cases of malicious allegations, the alleged party, or the employer, may consider legal action against an identifiable whistleblower.

Equally, as with many investigations, consideration must be given to the collection and recording of personal data. Legal advice should be taken on data protection obligations, as again, in some jurisdictions such as France, an accused person may be informed of the accusation and have a right of challenge when his or her personal data is recorded during a whistleblowing investigation.

With the protection of the whistleblower and disclosure obligations at the top of the investigator's priority list, it is important the internal investigation proceeds as with any other investigation to establish the facts. Establishing a dialogue with the whistleblower, if possible, allows for further information, context and feedback to take place. It can be that allegations are raised in good faith but are off-target owing to facts unknown to the whistleblower.

In the event the allegation, or allegations, are substantiated and lead to regulatory enforcement action, litigation by way of civil claims or criminal investigation, or all three, it may be that the identity of the whistleblower, if known, must be disclosed. Investigators should be mindful not to give whistleblowers definitive commitments of non-disclosure, even if authorities have whistleblower protections in place. In serious cases, this aspect requires early legal advice when the allegation is first received and assessed, as the legal risks will require consideration.

Everyone involved in the whistleblowing investigation and management process should remain aware that whistleblowers are free to speak to whomever they wish and this can include law enforcement, external regulators and taking their own external legal advice. Specialist legal advice should be taken in respect of employees who have raised concerns where the employer is considering reaching a settlement involving a non-disclosure agreement. Some jurisdictions consider these counterproductive to the aims of whistleblowing programmes. In the United Kingdom, the All Party Parliamentary Group on Whistleblowing[4] has called for legislation to ban the use of non-disclosure agreements for whistleblowers.

4 https://www.appgwhistleblowing.co.uk/.

22

Forensic Accounting Skills in Investigations

Glenn Pomerantz, Nicole Sliger and Michael Barba[1]

Introduction 22.1

The purpose of this chapter is to explain key steps and best practices in investigations from an accounting perspective. The term forensic, as defined in Webster's Dictionary, means 'belonging to, used in or suitable to courts of judicature or to public discussion and debate'. Accordingly, forensic accounting involves the application of specialised knowledge and investigative skills to matters in anticipation of possible litigation or dispute resolution, including in civil, administrative or criminal enforcement matters. Forensic accounting skills can be applied to a wide variety of investigations into alleged corporate and individual wrongdoing, including:

- misappropriation of assets by employees;
- bribery and corruption;
- money laundering;
- financial reporting fraud;
- non-compliance with laws, regulations or provisions of contracts; and
- fraud perpetrated by vendors or suppliers and other third parties.

We may refer to non-compliance instead of fraud. Non-compliance often lacks the intent of fraud and may manifest itself in the violation of an agreement, policy or otherwise acceptable behaviour. Investigations may focus on allegations of fraud or non-compliance.

The range of specialisations within the field of forensic accounting is diverse, but at the core is a focus on accounting systems, processes, records, data and

1 Glenn Pomerantz and Nicole Sliger are partners and Michael Barba is a managing director at BDO USA, LLP.

reports. A logical order in which forensic accountants will proceed in an investigation is as follows:

- gaining a broad understanding of allegations, accounting systems, employee responsibilities and business processes;
- preserving records and other evidence;
- mitigating losses;
- developing a workplan for the investigation;
- considering and carrying out data analytics, email review (often with counsel) and review of books and records;
- conducting (often with counsel) information-gathering interviews; and
- conducting (often with counsel) investigative interviews.

Many of the most important steps involved in this process are explained below.

22.2 Preservation, mitigation and stabilisation

See Chapters 5 and 6 on beginning an internal investigation

An important consideration at the outset of an investigation is to identify the necessary steps to mitigate loss of funds or other assets and to preserve data and relevant records. This may entail closing of bank accounts, freezing of email and other communications, deactivating user passwords and other steps to deny access to subjects of the investigation. Where the nature of the investigation requires it, financial and accounting information will need to be preserved and stabilised. Physical documents in this category may include a wide variety of records, such as purchase orders, invoices, customer orders, delivery records, etc. Every step of the transaction cycles involved in the scheme under investigation should be considered at this stage to identify all potentially relevant documents and electronic records (including audio).

22.3 e-Discovery and litigation holds

Owing to the proliferation of electronic data, an increasingly important early step in many investigations is to determine what relevant information exists, in what form (paper or electronic), where it is located (e.g., an on-site data centre, off-site at vendors, in the cloud), what security measures are in place over the data, and what the organisation's standard record retention and destruction policies and practices are. The process of identifying, taking inventory of, and preserving relevant data that may be of use in an investigation is often referred to as e-discovery.

In addition, as soon as it becomes apparent that an investigation is necessary, a litigation or preservation hold notice should be issued. These notices require the suspension of any destruction or deletion of paper or electronic records that could be relevant to the investigation. Proper communication of a litigation hold or preservation order to all pertinent individuals and department which may include third parties who, for example, are responsible for archiving the organisation's data off-site, is important to avoid accidental destruction of critical records.

Violation of internal controls 22.4

An important part of an investigation is establishing whether the act was intentional. Demonstrating that a subject was aware of and violated a documented, well-established internal control is often a relevant factor. For example, determining how an internal control was circumvented or otherwise violated is also an important part of understanding how fraud or corruption was perpetrated, because establishing that a subject intentionally violated internal controls can be important in connection with criminal prosecution or the regulatory enforcement process, and understanding precisely how internal controls were violated is critical to developing a remediation plan to enhance controls and to prevent future occurrences. In addition, understanding how internal controls were bypassed or overridden will often provide critical insight into who knew what and when.

The first step in determining whether policies or procedures were violated is to gain a thorough understanding of the accounting behind the controls as well as the identities of employees responsible for accounting, internal controls and the business processes being investigated. Upon gaining this basic knowledge, we identify the established policies and procedures (the current state). This normally entails reviewing documented policies and procedures, and walkthroughs, and may also include interviews with employees to help clarify any ambiguities in the documentation. Some considerations include:

See Chapters 7 and 8 on witness interviews

- which employees are authorised to initiate and process a transaction;
- which employees are authorised to approve a transaction;
- which employees can approve new vendors;
- which employees are responsible for account reconciliations;
- which employees have physical access to assets, including cash;
- documentation requirements for the transaction;
- how and where electronic and paper records are stored; and
- how exceptions or unusual transactions are handled, including budget variance analysis.

It may also be important to review any training programmes that the subject of the investigation has received. Doing so can establish more firmly that the subject had an understanding of the proper method of handling the transactions.

Most accounting cycles, such as procurement, disbursement of funds and payroll, include many steps. Some of these are evidenced manually, such as with written approvals by signature and supporting documents such as invoices and delivery confirmations. Other steps require analysis of electronic records. Examples of critical pieces of electronic evidence related to internal controls include:

- *Date and time stamps*: Most systems leave a valuable trail that can be used to establish an accurate and detailed timeline of events. For example, a vendor invoice may be put into the accounts payable system late at night during non-work hours, approved for payment moments later and payment is made to the vendor the very next day. Why the rush? Is there a legitimate need or is something more devious involved? Does payment so quickly comply with the organisation's normal cash management and bill-paying policies?

- *User identification numbers*: Systems maintain a record of user log-ins, along with date and time of information access and updates. Directly or indirectly, it is often possible to determine exactly which user of a system performed each step in the chain of activities comprising a transaction – who set a vendor up in the master file, who authorised the purchase and whether it was competitively bid, who entered the vendor invoice, who approved it for payment, who scheduled it for disbursement, who transmitted payment, etc.
- *Security matrices*: Often reviewed in connection with the preceding step, determining which users have access to specific components of each system can play a vital role in assigning responsibility for specific steps in a matter under investigation. Access to a system often does not mean access to every part of that system. Analysis of a security matrix provides details of this information. Who has 'read only' access to vendor and invoice data? Who has input capability? Who has approval authority to release payments to vendors? Aligning this information with information gleaned from the preceding steps can find exactly where internal controls were compromised, including identification of instances of unauthorised access through password theft or sharing.

Physical documents are often important pieces of evidence in an investigation. But electronic evidence associated with a transaction cycle tends to be equally or more important. Proper analysis of this evidence enables an investigator to draw conclusions and gain insight that would be impossible in an entirely paper-based system. For example, a paper copy of a vendor invoice can be analysed to establish whether a subject signed or initialled it, and perhaps whether any alterations were made to the document. But if the organisation's vendor invoice approval and payment system is electronic, the investigator can also determine with precision the date and time of the approval of the invoice and perhaps even where the subject performed these steps (from home, from a workstation in the office, etc.).

22.5 Forensic data analysis

Forensic analysis of data refers to analysis of electronically stored data. The most commonly analysed data are accounting and financial, but several non-financial categories of data are also very useful to investigators. Each is explored below.

Data analysis generally has three applications in the investigative process:

- to initially detect fraud or non-compliance (e.g., monitoring performed by internal audit);
- to corroborate an allegation in order to justify launching an investigation (e.g., proving that an allegation received via a hotline appears to have merit); and
- to perform certain parts of the investigation (e.g., analysis of payments made to suspicious vendors).

Each of these will be explained further. But first, a few important points about data analytics are essential.

Data analytics rarely prove that fraud or non-compliance occurred. Rather, data analysis identifies transactions or activities that have the characteristics of fraud or non-compliance, so that they can be examined further. These are often referred to as anomalies in the data.

If an investigation ultimately leads to employee terminations or legal proceedings to recover losses, it is critical to have properly analysed the anomalies that data mining has identified. Could the anomaly in the data, or an anomaly in a document, while often identified as a characteristic of fraud, also simply indicate a benign deviation? Failing to investigate and rule out non-fraudulent explanations for anomalies can have consequences that many investigators have learned about the hard way.

Identifying and exploring all realistically possible non-fraudulent, non-corrupt explanations for an anomaly is also called reverse proof. Examining and eventually ruling out all of the valid possible non-fraudulent explanations for an anomaly in the data or documentation can prove that the only remaining reasonable explanation is fraud or corruption.

Take a simple example to illustrate this important concept. An employee is found to have submitted the same business expenditure twice for reimbursement (paid for using a personal credit card). Further analysis shows that this is not an isolated incident. In fact, the rate at which the employee submitted duplicate expenditures has increased over time – a classic red flag commonly associated with perpetrators of fraud. Is this a sufficient basis to support an allegation of misconduct?

This would be premature. What if, on further analysis, the investigator also finds that the employee has been asked to work an increasing number of hours every week and travel much more extensively over time. Investigating further, it is found that this employee is particularly disorganised and has never been asked to do this much business travel before. These additional facts make the distinction between an intentional act of fraud and an escalating series of honest mistakes a bit blurry.

Careful consideration of alternative theories for data and document anomalies is critical to protecting the organisation and the investigator from liability stemming from falsely accusing someone of wrongdoing.

Data mining to detect fraud or non-compliance 22.5.1

Depending on which application or phase of the investigative process is involved, the nature of forensic data analysis can vary. For example, as an initial detector of fraud or non-compliance through ongoing monitoring, forensic data analytics usually takes one of two broad, but opposite, approaches: identification of any activity that deviates from expectations, or identification of activity that possesses specific characteristics associated with fraudulent or corrupt behaviour or other non-compliant conduct.

The former approach is taken when acceptable behaviour is narrowly defined, such that the slightest deviation warrants investigation. The latter approach is the more common. It is driven by a risk assessment and is based on what this type

of fraud or non-compliance would look like in the data. For example, a shell company scheme might evidence itself by an address in the vendor master file matching an address in the employee master file. Any instances of such a match would be investigated.

In some cases, basing the 'investigate' or 'don't investigate' decision on a single characteristic in the data can result in numerous false positives. For this reason, more sophisticated data analytics often rely on the consideration of multiple characteristics in assessing the risk of activity being fraudulent or corrupt.

Regardless of which of these two approaches is taken, data analytics often represents an essential tool for gathering evidence to lay the foundation for substantive examination of books, records and other evidence. Following the reverse-proof concept described above is critical once anomalies indicative of possible wrongdoing are uncovered.

22.5.2 Corroborating allegations

See Chapters 19 and 20 on whistleblowers

As a method of corroborating an allegation that has been received, data analysis can be of great value. It is a significant advantage to the investigator because, more often than not, it can be performed on electronic data without alerting the subject of the allegation. In this application, the allegation is first assessed in terms of what impact the alleged fraudulent or corrupt act would have on financial or non-financial data. To illustrate, take the example of an allegation that workers in the shipping department of a warehouse are stealing inventory by short shipping orders to customers. There are numerous sources of data, both financial and non-financial, that could be analysed to assess the validity of this allegation:

- gross profit margins – an unexplained decline in gross profit margins by product, or by location (as a result of having to re-ship additional items, with no associated revenue, to satisfy the customer);
- inventory purchases – unexplained increases in purchases of certain inventory items without a corresponding increase in sales;
- customer complaints – customer service data indicating complaints about incomplete shipments, especially if those complaints can be correlated back to specific orders; and
- shipping records – using the customer complaint data, orders are correlated to specific shipments and employee names associated with filling and shipping these orders. Shipping records might also reveal more shipments to a customer than orders, indicating a second shipment was needed to complete the order after the customer complained.

This is a simple example, but one that illustrates that for every allegation, there likely exists data associated with either the perpetration or concealment of the fraud or non-compliance. And this data normally exhibits one or more anomalies in comparison with data from similar transactions that do not involve fraud or non-compliance.

Using data analysis in an investigation 22.5.3

The final application of forensic data analysis is performed during the investigation itself. Once an anomaly has been found to involve fraud or non-compliance, additional forensic data analysis, along with substantive forensic examination of the evidence, may be performed to:

1 determine how long the activity has occurred;
2 determine which employees (or third parties) have participated in the fraud (i.e., assessing whether collusion was involved);
3 measure the financial damage resulting from the activity;
4 identify other fraudulent or corrupt conduct by the same individuals; and
5 determine how the fraudulent or corrupt act was concealed and how internal controls were circumvented.

Determining who is involved in the fraud as well as who possessed knowledge of it is critical to the mitigation and control enhancement objectives. According to a 2016 report by the Association of Certified Fraud Examiners (ACFE), nearly 45 per cent of all fraud and corruption schemes investigated involve multiple perpetrators.[2] This figure has been steadily rising since the ACFE began studying fraud. The 45 per cent is split nearly evenly between cases involving multiple internal perpetrators and those involving collusion between insiders and outsiders, such as vendors or customers.

Point 4, above, may also come as a surprise to some, but is important. The ACFE report indicates that 31.8 per cent of the time an individual engages in fraud (especially with respect to asset misappropriations), they employ multiple methods to commit their crimes. The allegation or investigation may have initially focused on only one specific method. Exploring what other activities the subject might have the capability of engaging in is an integral element of the investigation. Investigators and victims attempt to 'put a fence around the fraud' as early in the investigative process as possible. Understanding the responsibilities of the subject and the potential for unrelated schemes is essential for erecting the fence. Victims often desire a narrow investigative scope – a sort of wishful thinking. An investigator's worst-case scenario is missing a scheme conducted by a subject despite investigating the subject.

The question of who knew what and when can be particularly important in satisfying auditors in the context of financial reporting fraud. In addition to quantifying the financial statement impact from fraud, auditors rely on representations from management. Knowledge of whether previous representations came from fraudsters and the auditor's assessment of management's integrity are often important aspects of financial reporting fraud investigations.

In the next sections, the distinction between financial and non-financial data will be explored, followed by a discussion of internal versus external data.

2 2016 ACFE Report to the Nations on Occupational Fraud and Abuse, published by the Association of Certified Fraud Examiners. Available at http://www.acfe.com/rttn2016.aspx.

22.6 Analysis of financial data

Most analyses of internal data relevant to an investigation begin with financial data, much of which comes from the organisation's accounting system. Accounting data can exist in several separate systems, such as:

- general ledger, the master ledger that reflects all accounts and the sum of all accounting activity for the organisation;
- general journal, where journal entries are initially recorded before being posted to the general ledger;
- books of original entry, which contain details of certain types of financial transactions, summaries of which are posted to the general ledger. Examples of books of original entry include sales, cash receipts, cash disbursements and payroll; and
- subsidiary ledgers, which contain additional details of transactions and activities that appear only in summary form in the general ledger. Examples of subsidiary ledgers are accounts receivable and accounts payable ledgers.

Performing an investigation often requires the extraction and analysis of data from all these systems to see the big picture or to properly trace the history of a transaction or series of activities. The days of manually maintained books of original entry are gone. The vast majority of organisations now use electronic accounting and financial software, and in larger organisations these systems are included as part of a broader ERP system.

Some systems are hybrids of financial and non-financial information. Examples of these systems include:

- *Inventory*: in addition to cost information associated with purchases, the system may also provide data on quantities and dates of purchases, deliveries, shipments, inventory damaged or scrapped, and counts resulting from physical observation.
- *Payroll*: in addition to data on net amounts paid to employees, the payroll system will usually include other relevant data needed to calculate an employee's gross and net pay, including various worker classification codes, hours worked during a pay period, rates of pay, tax and withholding information, along with bank account information for the electronic transfer of funds to employees.
- *Human resources*: in most large organisations a human resources system that is separate from payroll is maintained. Included in this system are data on rates of pay and past raises, incentive payments, and other financial data about each employee, as well as significant amounts of non-financial data, such as each employee's home address. Human resource information systems may also include vital information associated with an employee's initial hiring, such as background and reference checks, verification of information provided on an employment application, etc. This information can be important if the organisation anticipates filing an insurance claim to be indemnified for losses attributable to an employee.

Availability of and legal considerations associated with each of these sources of internal data vary from one jurisdiction to another, particularly with respect to payroll and personnel information. Privacy issues must be considered before embarking on any use of such data in an investigation.

Analysis of non-financial records 22.7

Increasingly, non-financial data is being analysed as a standard element of an investigation. Non-financial data can be classified into two broad categories: structured and unstructured.

Structured data is the type of data that generally conforms to a database format. It is often numeric (e.g., units in inventory, hours worked by an employee, calendar dates), but can involve alpha data as well (e.g., codes associated with types of customer or employee, certain elements of an address).

Structured non-financial data is found in many systems, including those that include financial data mentioned above. Other systems, however, are entirely non-financial, but provide data that can be important to an investigation. Examples of non-financial systems commonly used for investigative purposes include:

- *Security*: many organisations now use tools that leave an electronic trail of the exact times and dates when specific employees entered or left the building. Records of visits by vendors and other visitors may be included in this system or may be kept separately. Security information can be very useful in establishing timelines or the whereabouts of specific individuals.
- *Network data*: much like accessing a building, networks maintain electronic records each time an authorised user logs on or off the system, and may retain a record of various aspects of the user's network activity, such as which folders were accessed, which data was downloaded, which systems were used, etc.
- *Customer service*: as the earlier example illustrates, data collected in the customer service system can have numerous applications in an investigative setting. Customer complaints about items missing from their orders may indicate theft in the warehouse.

Unstructured data refers to data that does not readily conform to a database or spreadsheet format. Text associated with messages in emails, explanations for journal entries and other communications are the most common. Unstructured data also includes photographic images, video and audio files.

Emails and text messages of interest to an investigator may involve messages within the organisation, between employees and communications between organisation employees and vendors, customers or other third parties.

Similar to other electronic data, when a user 'deletes' this information, a backup or archive version is often left behind and is available to an investigator. Understanding an organisation's backup, archiving and storage practices is crucial to this part of an investigation.

Careful reviewing of email, instant messaging or text message chains (and, if available, recordings of telephone calls) is vital to most investigations and can provide an investigator with vital clues, such as:

- the timeline of events;
- the level of knowledge of events that specific individuals may have had;
- the extent of collusion among individuals;
- whether a subject or witness deleted email evidence; and
- whether there are indications of intent.

Establishing a timeline can be one of the most important requirements of an investigation. A complete timeline of events can often be established by integrating the separate timelines learned from a review of:

- systems and facilities access records;
- electronic transaction information (e.g., entries, approvals);
- documentation (e.g., invoices, shipping records); and
- electronic communications, including metadata (e.g., emails).

Email (and where available, audio) review is of particular importance in establishing intent. Intent, particularly to a civil standard, may be inferred from communications that indicate an awareness that planned transactions or activities are in conflict with established policies and procedures or treatment of similar transactions. Sentiment analysis can also be performed in connection with email, instant messaging or text message communications. This type of analysis can identify pressures or rationalisations associated with fraudulent or corrupt behaviour. For example, an employee stating in these communications that he or she feels unfairly treated or resentment towards management might be expressing a rationalisation for stealing from an organisation.

One example of the use of both financial and non-financial data is in the investigation of alleged financial reporting fraud. When an allegation is made that a company's financial statements have been intentionally manipulated, any of a large number of schemes come to mind. The most common fraudulent financial reporting schemes involve improper recognition of revenue, inflating turnover or sales through fictitious transactions or accelerating the recognition of legitimate transactions. So, a revenue inflation scheme will serve as our example.

To establish that the financial statements improperly reflect sales, electronic data from the sales and accounts receivable systems will need to be analysed in conjunction with physical or electronic records associated with customer orders, inventory, shipping and delivery, among others. By analysing these records, the investigator may establish that sales recognised by the company failed to conform to applicable accounting standards (e.g., International Financial Reporting Standards).

But accounting mistakes are common. For this scheme to be fraudulent, the subjects' dishonest intent to violate the accounting rules must be established. This is where analysis of emails and other electronic communications may be valuable. Perhaps email exchanges can be located documenting discussions of

revenue shortfalls and methods of meeting budgeted figures. In this case, analysis of unstructured non-financial data may be one of the keys, along with interviews of subjects, to proving that the company intentionally violated their own policies and pertinent accounting principles.

Analysis of both financial and non-financial data is an important step in preparing to interview witnesses and subjects. Reading email and other communication chains before conducting the interview allows an investigator to plan the order and structure of questions to put the interviewer in the best position to identify conflicting statements and to obtain a confession.

Other investigation scenarios in which analysis of unstructured data association with communications between individuals include:

- collusion between multiple employees involved in the theft of cash or other tangible or intangible assets;
- bribery schemes in which the organisation has paid bribes, directly or indirectly, to obtain or retain business; and
- kickback schemes in which a vendor has paid a procurement official of the organisation to steer business to the vendor.

Use of external data in an investigation 22.8

Most data and documentation used in an investigation is internally generated – it comes from within the organisation or (in the case of invoices from a vendor) is otherwise readily available within the organisation. Occasionally, however, data or documentation that is only available from external sources becomes essential. External sources of data fall into two broad categories, public and non-public.

Public data and documents are those that are usually available to the general public either by visiting a website or facility or on request from the holder of the records. In most cases, public records are maintained by government agencies. Examples of public records vary significantly from one jurisdiction to another, but some that may be useful to investigators are:

- licences and permits issued by government agencies to individuals or businesses;
- records of ownership or transfers of ownership of property (e.g., sales of land and buildings);
- criminal convictions of individuals and organisations, and certain other court records; and
- business registrations and certain filings made by organisations.

Availability and the extent of these records can differ markedly as an investigator seeks information from different parts of the world.

Increasingly, public records may also include information that an individual voluntarily makes publicly available. For example, when an individual posts photos or makes statements on social media, this information might be readily available to any and all viewers. Once again, investigators should always use caution when accessing this information, especially if the information is only available to 'friends' or other contacts that the individual has granted special access to. But

when social media information is made fully available to the general public, it can provide a treasure trove of information about a subject, such as:

- places the subject has visited;
- individual contacts;
- business relationships;
- assets owned; and
- past and present employers.

Another public source of information involves websites that do not require special password or other access privileges. For example, a company's website or that of a trade association or other membership group that a subject might be involved with could provide clues about the subject's relationships, travels and past.

Even information that is no longer on a website might still be available to an investigator. The Wayback Machine at www.archive.org is an archive of almost 500 billion past pages on the internet. Simply typing the URL of a website into the Wayback Machine will produce an index by date of prior versions of that website which have been archived and are available for viewing. Accordingly, an investigator may be able to find useful information from past editions of websites long after the information has been deleted.

Non-public records are private and confidential. Holders of these records are under no obligation to produce these records unless they have provided their consent or they are compelled to do so as a result of a legal process, such as a court order or subpoena. Records such as personal bank statements of individuals who may be the subject of an investigation fall into this category. Investigators normally do not have ready access to these records.

When assisting counsel with preparing a request for a subpoena or other court-ordered production of private records, an investigator should be as detailed and specific as possible. Overly broad requests are normally either denied or result in potentially lengthy delays. For example, if records associated with a bank account are requested, rather than requesting 'all records associated with the account', it is normally better to itemise a list of those records, such as by requesting copies of:

- bank statements for the relevant period;
- images of cleared checks;
- supporting documents for other debits from the account;
- signature cards; and
- application or other forms prepared to open the account.

A vendor's internal records would normally be non-public and the vendor may be under no obligation to provide them to an investigator. However, a properly worded right to audit or access to records provision included in the contract between the organisation and the vendor may provide access to some of the most important records an investigator might need if fraud or corruption involving a

vendor is suspected. A well-crafted access-to-records clause can enable an investigator to request and view a wide variety of records, including:

- supporting documentation for invoices sent to the organisation by the vendor;
- accounting and payroll records;
- time records supporting employees' work efforts; and
- communications relevant to the vendor's relationship with the organisation.

If a vendor is suspected of inflating their billings to the organisation in any manner, or there are indications of collusion between an organisation employee and a vendor, one of the first steps an investigator should perform is to carefully review the terms of the contract to assess the organisation's rights to access these records.

Review of supporting documents and records 22.9

Studying the processes and internal controls involved in the transaction cycle in the investigation and the results from data analytics and email review will result in a population of documents and electronic records that are relevant. For example, in a corruption investigation, several paper documents or records may need to be reviewed:

- budgets;
- agent, distributor, supplier and customer contracts;
- bidding documents;
- margin data;
- price lists;
- market data;
- vendor set-up documents;
- sales by region, agent, territory and product;
- background checks;
- purchase order or purchase request;
- bill of lading or other confirmation of delivery of goods;
- signed confirmation for services provided;
- invoice from a vendor or supplier;
- cheque or disbursement request form; and
- banking records.

These records might be reviewed for many different reasons. Among the most common are:

- establishing a timeline of events;
- testing their clerical accuracy;
- reviewing for inconsistencies, anomalies and trends;
- reviewing for agreement with accounting records;
- reviewing for compliance with internal controls; and
- determining authenticity of the document, the vendor and the services rendered.

Testing for authenticity of the record itself or of individual signatures on documents normally involves a highly specialised skill, unless an anomaly is obvious. Accordingly, if an investigator suspects that a document on file is fraudulent or has been physically altered, or that a signature is not authentic, the document should be protected until someone with the specialised skills necessary to assess authenticity is called on. Examples of obvious deficiencies in documentation include:

- inconsistencies in addresses;
- lack of letterhead or other characteristics normally expected of a legitimate vendor;
- misspellings or other typographical errors;
- document at variance with vendor master file;
- inconsistencies in dates; and
- inconsistencies in vendor invoice numbers and sequencing.

In a corruption investigation, the authenticity or business purpose of an intermediary may be in question. The investigator should determine:

- the purpose of the intermediary;
- the principals behind the intermediary;
- the value, if any, of services rendered by the intermediary, to rule out use of the intermediary to create a slush fund or otherwise bribe a customer or influencer;
- life before or after the intermediary; and
- if the company documentation in connection with the intermediary is consistent with other intermediaries, policies and best practices.

22.10 Tracing assets and other methods of recovery

If the subject has misappropriated cash (via intercepting incoming funds intended for the organisation, stealing cash on hand, or fraudulently transferring funds from the organisation in connection with a disbursement fraud) one of the goals of most investigations is to secure the return of the funds. To do so, the investigation team must determine what the subject did with the money. Other sources of recovery may include culpable outside parties, including but not limited to collusive vendors, customers and agents. Coverage for employee dishonesty losses under insurance policies and fidelity bonds may also be possible.

If the subject misappropriates other assets, a similar question must be addressed – where are they? Often, when assets are stolen, the subject's goal is a conversion to cash by selling the stolen assets. In other cases, the stolen asset itself may be of use to the subject.

Depending on how assets were stolen, varying degrees of a trail might be left by the perpetrator, enabling the investigation team to forensically determine the flow of money after it has left the organisation. The trail may begin with the company's books and records. However, it is usually intentionally made opaque by fraudsters through money laundering techniques such as layering, transfers to shell companies, nominee shareholders and the use of clandestine communication techniques, cryptocurrencies, and tax havens where criminal law enforcement assistance may be less effective. Many of the records necessary to fully trace assets

are non-public. But investigators are sometimes surprised to learn that a subject has left a public trail of valuable clues regarding the disposition or location of illegally obtained funds or assets that can be identified through indirect techniques, such as social media and internet due diligence, interviews of people in the know, establishing connections to the fraudster's other assets in more vulnerable venues and through multinational co-operation of law enforcement agencies.

Development bank forensic audit 22.11

One setting where forensic accountants have increased their presence in recent years is in forensic audits[3] in connection with multilateral development banks.

Multilateral development banks such as the World Bank Group, Inter-American Development Bank (IDB) and Asian Development Bank (ADB), have investigative offices within their organisations known as integrity departments.[4] Each of these integrity departments differs in name – Integrity-Vice Presidency (World Bank), Office of Institutional Integrity (at the IDB), Office of Anticorruption and Integrity (at the ADB) – but they share a similar mandate: the investigation of allegations of sanctionable practices within the scope of the broader development agenda of each bank.[5] These development banks have harmonised their anti-corruption principles and share many investigative approaches.[6] Since the purpose of these investigations is to determine the merits of allegations of corrupt and fraudulent practices, with the standard of proof being preponderance of the evidence, they are also an integral tool used more broadly in the oversight and mitigation functions of multilateral development banks. One senior forensic

3 A forensic audit is the application of specialised knowledge and investigative skills used to collect, analyse and evaluate evidential matter and to interpret and communicate findings in the courtroom, boardroom or other legal or administrative venue (Durkin and Ueltzen, 2009).

4 Other multilateral development banks also have integrity departments. These include European Bank for Reconstruction and Development, African Development Bank, European Investment Bank and Asian Infrastructure Development Bank, but for the purpose of this chapter, the writers are limiting their comments to the World Bank Group, Inter-American Development Bank and the Asian Development Bank.

5 World Bank, 'Annual Update Integrity Vice Presidency Fiscal Year 2017', http://www.worldbank.org/en/about/unit/integrity-vice-presidency (last accessed 20 August 2018); World Bank, 'Who We Are', http://www.worldbank.org/en/who-we-are (last accessed 20 August 2018); Inter-American Development Bank, '15 Years Standing Against Corruption', Office of Institutional Integrity and Sanctions Systems, 2017 Annual Report, http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=EZSHARE-1138756496-150 (last accessed 24 August 2018); Inter-American Development Bank, 'About Us', https://www.iadb.org/en/about-us/overview (last accessed 24 August 2018); Asian Development Bank, 'iACT for Integrity and Respect Office of Anti-corruption and Integrity 2017 Annual Report', https://www.adb.org/sites/default/files/institutional-document/408321/oai-ar2017.pdf (last accessed 24 August 2018); Asian Development Bank, 'Who We Are', https://www.adb.org/about/main (last accessed 24 August 2018).

6 Asian Infrastructure Investment Bank, 'AIIB Yearbook of International Law: Good Governance and Modern International Financial Institutions', https://www.aiib.org/en/about-aiib/who-we-are/yearbook/index.html (last accessed 22 August 2018); Asian Development Bank, 'Integrity Principles and Guidelines (2015)', https://www.adb.org/documents/integrity-principles-and-guidelines (last accessed 24 August 2018).

accountant from the World Bank noted the significance of forensic accounting in the bank's oversight function and its use to proactively reduce financial losses.[7] Moreover, in the World Bank's Integrity Vice Presidency's 2017 annual report, the forensic services unit conducted a total of 13 audits involving 19 entities and 31 contracts valued at more than US$518 million.[8] This annual report noted that 'forensic audits' were also utilised to strengthen the World Bank's fiduciary role and for risk management, in particular on the riskier projects.[9] In its 2017 annual report, the IDB's Office of Institutional Integrity noted its audit and inspection powers in its investigations. The IDB also alluded to the 'forensic audit' as an investigative tool.[10] Although the ADB's Office of Anticorruption and Integrity 2017 annual report did not cite forensic audits or inspection rights as an investigative tool, as discussed further below, the ADB in fact also has similar audit and inspection rights.[11]

The possible upshot of the significance of forensic accounting and exercise of audit and inspection rights in these multilateral development banks' investigation and oversight functions is that forensic accounting will continue to evolve and is likely to become one of the most valuable tools to protect their policies.

Procurement guidelines and inspection clauses

The procurement guidelines or policies from the World Bank, IDB and ADB in general state that all borrowers, bidders, suppliers, consultants and contractors must observe the highest ethical standards.[12] The purpose of these high standards is to ensure that these parties will not be involved in sanctionable practices such

7 Ferlatte, Ryna, 'Fighting corruption behind the scenes: The evolving and ever important role of forensic audits in international development', People, Spaces, Deliberation, World Bank, 13 May 2016, http://web.worldbank.org/archive/website01603/WEB/FIGHTING.HTM (last accessed 13 November 2019).

8 World Bank, 'Annual Update Integrity Vice Presidency Fiscal Year 2017', http://www.worldbank.org/en/about/unit/integrity-vice-presidency (last accessed 20 August 2018).

9 Ibid.

10 Inter-American Development Bank, '15 Years Standing Against Corruption', Office of Institutional Integrity and Sanctions Systems, 2017 Annual Report, http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=EZSHARE-1138756496-150 (last accessed 24 August 2018).

11 Asian Development Bank, Procurement Guidelines (April 2015) and Asian Development Bank, Guidelines on The Use of Consultants by Asian Development Bank and its Borrowers (March 2013).

12 World Bank, Guidelines: Procurement of Goods, Works, and Non-Consulting Services under IBRD Loans and IDA Credits & Grants by World Bank Borrowers (January 2011, revised July 2014) and World Bank Guidelines: Selection and Employment of Consultants under IBRD Loans and IDA Credits & Grants by World Bank Borrowers (January 2011, revised July 2014); Inter-American Development Bank, Policies for the Procurement of Goods and Works financed by the Inter-American Development Bank GN-2349-9 (March 2011) and Inter-American Development Bank, Policies for the Selection and Contracting of Consultants financed by the Inter-American Development Bank (March 2011); Asian Development Bank, Procurement Guidelines (April 2015) and Asian Development Bank, Guidelines on The Use of Consultants by Asian Development Bank and its Borrowers (March 2013).

as corrupt, fraudulent, coercive and collusive practices.[13] Within the context of these anti-corruption clauses, these procurement or policy guidelines also provide that a provision is required to be included in the request for proposals (or bidding documents) and any subsequent contracts that would permit the respective Banks to inspect documents related to the submission of proposal (or bids) and contract performance.[14] For example, the IDB's procurement policies provide for the insertion of an inspection clause, 'to permit the Bank to inspect any and all accounts, records and other documents relating to the submission or proposal (bid) and contract performance, as well as to have them audited by auditors appointed by the Bank.'[15] This clause provides for potential inspection or audit to be very broad in scope. The guidelines and policies from the World Bank, IDB and ADB provide no definitions or clarifications as to what specific accounts, records or other documents should be part of inspections and audits.[16]

When these inspection clauses are exercised during investigations by the integrity departments at these banks as part of their broader investigation against bidders, suppliers, consultants and contractors for alleged violations of sanctionable practices, a forensic accountant potentially has a wide latitude to review all kinds of financial documents, namely bank statements, tax invoices and vouchers. The senior forensic accountant at the World Bank mentioned above said that some of the World Bank forensic audits begin with complaints received by their integrity department and that, most commonly, their forensic audits reveal patterns of procurement fraud, conflict of interest, self-dealing, kickbacks, fraud in implementation and embezzlement of project funds.[17] In such cases, professional accounting skills coupled with an investigative mindset are used to uncover the misconduct.[18]

In summary, the forensic auditing of multilateral development banks as well as advising on the prevention, detection and mitigation of fraud and corruption constitute a significant growth area for forensic accountants.

Investigations involving national security interests 22.12

Forensic accountants engaged on investigations that involve national security interests require heightened sensitivity. Forensic accountants may find themselves involved in engagements where state secrets are either an integral or a tangential part of the assignment. For example, engagements related to the Committee on

13 Ibid.

14 Ibid.

15 Inter-American Development Bank, Policies for the Procurement of Goods and Works financed by the Inter-American Development Bank GN-2349-9 (March 2011) and Inter-American Development Bank, Policies for the Selection and Contracting of Consultants financed by the Inter-American Development Bank (March 2011).

16 Ibid.

17 Ferlatte, Ryna, 'Fighting corruption behind the scenes: The evolving and ever important role of forensic audits in international development', People, Spaces, Deliberation, World Bank, 13 May 2016, http://web.worldbank.org/archive/website01603/WEB/FIGHTING.HTM (last accessed 13 November 2019).

18 Ibid.

Foreign Investment in the United States (CFIUS), cross-border investigations or those involving entities employing a cross-border investment strategy may also, by their nature, involve intellectual property secrets of US companies who are contracted by the US government. This information may also be defined by CFIUS as 'protected data' in that any inadvertent or malicious release of this data can impact the national security of the United States. Several other types of engagements, including US Foreign Corrupt Practices Act investigations, international arbitrations and monitorships may present state-secret issues while not representing the core of the matter.

As technological innovation continues to dictate the rules of modern-day business, forensic accountants investigating entities employing a cross-border investment strategy should be cognisant of the complexities and heightened risks that arise due to national security interests. Special consideration should be given to the following emerging issues when dealing with companies that potentially pose national security risks.

22.12.1 IT infrastructure and potential segregation of client data

Forensic accountants should develop a customised risk profile at the onset of the investigation to assess possible cyberthreats, gaps in firm IT infrastructure controls, intrusion points and other high-risk scenarios. Subject to local law restrictions, the investigative team should consider separating physically and logically any client data received to prevent potentially virus-ridden files or malicious codes from being introduced or injected into firm networks. For example, consider using stand-alone servers with remote access (e.g., a Citrix environment) to review documents and conduct normal business activities during the investigation.

These safeguards, however, must be weighed against the practicalities of how the forensic accountants conduct their work – a careful balance needs to be struck between being vigilant and creating inefficiencies for the investigative team. Additionally, the views of the investigative team members should be taken into account – despite having the appropriate policy or protocols, a risk exists that they may be ignored if viewed by the engagement team members to be too strict or rigid. To the extent possible, less complex, user-friendly protocols should be implemented to encourage compliance, for example, the use of computers or devices with built-in heightened security features. Engagement teams may also consider implementing a cyber management centre operating round the clock to monitor and support the field team to lessen the burden on individuals.

While these options may be costly, it may be the most prudent approach to protect the investigative team from cyberthreats.

22.12.2 Compliance with data privacy laws and state secrecy law

Investigative teams should engage legal and IT infrastructure specialists experienced in navigating data privacy and state secrecy law issues to assist them with developing the appropriate protocols to ensure compliance. The specialists should have specific knowledge and experience of the local laws and regulatory authorities in the countries involved in the investigation. Forensic accountants should be

cognisant that even the company under investigation may not have the authority to determine whether the information and data being provided to them in the normal course of its investigation is considered a state secret. It is important not to rely solely on the company's corporate legal and IT departments to make such determinations.

Nonetheless, forensic accountants should obtain written confirmation from the company under investigation explicitly stating that no state or commercial secret information is being provided, or to the extent it is, the company has obtained the appropriate authorisation to share such information. Furthermore, additional precautionary measures such as entering into confidentiality agreements for information exchanges should be considered.

Without external legal and IT infrastructure specialists, serious repercussions and risks potentially exist for the engagement team, including but not limited to possible arrest, detainment, etc. Depending on the nature of the investigation and the risk profile of the countries involved, the investigative team should develop a contingency plan and emergency protocol in the event a team member is detained, arrested or otherwise compromised.

Involvement of foreign nationals 22.12.3

If the engagement requires assistance from foreign nationals, the forensic accounting team should consider implementing safeguards to limit access to potentially sensitive documents to prevent unauthorised or inadvertent sharing of information. Any potentially sensitive documents should be shared on a 'need to know' basis and appropriately segregated from other engagement data and documents. Depending on the risk involved, certain engagements may, for example, necessitate compartmentalising any foreign national team member's access to systems to prevent 'insider threat' scenarios. While the foreign national team members themselves may not pose any imminent threat individually, their access to the data and the inner workings of the investigative team may subject them to be targeted by the intelligence services of the foreign country who may have a vested interest in the investigation.

Careful consideration should be given to the assigned roles and responsibilities of any foreign nationals. Additionally, forensic accountants should consider designating an engagement team coordinator to manage and track activities of foreign nationals to mitigate risks.

Use of translators 22.12.4

Forensic accountants should exercise caution when using translators on its investigations involving national security concerns. Translator candidates should undergo a full scope background check prior to being engaged to identify potential areas of concern (e.g., former media reporters, prior government employment, ties to other parties of interest). Additionally, it is not uncommon for embassies and other foreign government agencies to engage translators for their own purposes – potentially from the same translation vendors as the investigative team. As such, an increased counterintelligence risk exists. The forensic accounting team should

develop specific protocols in regard to sharing information with translators providing them with only the basic information needed to perform their duties (e.g., brief background, objectives, specialised terms). The engagement team should avoid broader discussions on investigation planning or findings and observations when translators are present, to limit the potential risk of infiltration.

22.12.5 Countries with advanced intelligence gathering capabilities

Investigations involving countries, such as Russia or China, with advanced intelligence gathering may pose an increased risk to friends and family members of the engagement team and engagement vendors or contractors. It is not uncommon for the intelligence agencies of such countries to make contact with individuals associated with highly sensitive investigations to collect any intelligence available. Forensic accountants should consider imposing a strict travel protocol to prevent team members from having contact with foreign nationals or even friends and family residing in the countries where the company under investigation has a presence to avoid any unnecessary risks. Moreover, the investigation team should frequently reiterate the importance of confidentiality throughout the investigation to deter inadvertent leakage of information.

22.12.6 Companies with significant state support

Investigations into companies that receive significant state support may pose additional risk for engagement team members. Nation states could potentially target the investigation for surveillance. As such, forensic accountants should consider engaging counterintelligence professionals to assist from an engagement planning perspective. For example, investigative teams may consider engaging security professionals to perform due diligence on hotels and other locations to be frequented by the engagement team. Additionally, security professionals can assist with developing travel protocols, including best practices such as using the 'buddy system' (i.e., never travel alone), keeping a low profile and limiting travel within designated safe areas.

22.12.7 Foreign investment and particular US national security concerns

In addition to the foregoing engagement-specific considerations, forensic accountants should also be generally familiar with the impact of foreign investments in the United States and how those investments are viewed by the US government as a potential threat to national security. Although forensic accountants may not have any specific charge to review such foreign investments in conducting their work, their investigative procedures may reveal a percentage of foreign funds invested in US companies that constitutes 'control' of the company under investigation. CFIUS oversees the national security aspects of foreign direct investment in the US economy. Forensic accountants may have an obligation to report findings regarding foreign control to a company's general counsel to ensure awareness of the CFIUS regulations. The company's general counsel would then decide whether to file a voluntary notice with CFIUS.

Forensic accountants should be aware that CFIUS's purview now expands well beyond the common critical infrastructure industries, such as aerospace and defence, and other US government contractors that support US government agencies since President Trump signed into law the bipartisan Foreign Investment Risk Review Modernization Act in October 2018. The intensified scrutiny of certain industries expanded CFIUS's purview and designated 27 new 'critical technology' sub-industries.

CFIUS can no longer be an afterthought. Forensic accountants should recognise that investors are considering CFIUS reviews as a priority. Recent regulatory updates have empowered CFIUS to intervene much earlier in the investment transaction negotiation process. As a result, legal teams for potential foreign investors who are seeking to invest in certain US industries no longer question whether CFIUS should be involved, but rather how, and how early.

Conclusion 22.13

The rapid conversion of accounting and other records from paper-based systems to electronic systems, coupled with the explosion in the quantity and types of electronic data, has resulted in many changes in the field of forensic accounting and the requirements for investigations. Expertise in the evaluation and handling of electronic evidence is just one way in which forensic accounting has evolved. Focused and efficient use of data analytics as well as the ability to mine a universe of publicly available yet critical information regarding subjects, companies and their relationships are two additional ways in which forensic accounting has matured. On the other hand, operating within a web of global data privacy and other complex regulatory constraints can complicate the job of the forensic accountant. All in all, today's forensic accountants are significantly more successful in identifying, investigating and mitigating fraud than their counterparts in the past.

23

Negotiating Global Settlements: The UK Perspective

†**Rod Fletcher and Nicholas Purnell QC**[1]

23.1 Introduction

This chapter discusses the three main options that corporates typically consider when they are seeking to settle criminal and related proceedings in England and Wales – negotiated plea agreements, civil recovery orders (CROs) and, as of 24 February 2014, deferred prosecution agreements (DPAs).

Central to any consideration of criminal settlements in England and Wales is the identification principle under the common law, which defines the scope of corporate criminal liability. The principle states that the 'acts and state of mind' of only those who represent the 'directing mind and will' of the corporate will be imputed to it.[2] The application of this principle is generally restricted to the actions of the board of directors, the managing director and other senior officers carrying out managerial functions and acting and speaking as the corporate.[3] Historically, the identification principle has made it very difficult for authorities in the United Kingdom to convict corporates of any significant size. The English courts have, in certain situations, applied this rule of attribution to persons outside the board level, but this will depend on the construction of the particular offence in question.[4] This relatively narrow position should be contrasted with that in the United States, where corporates may be vicariously liable for the acts

1 Rod Fletcher was a partner at Herbert Smith Freehills LLP until his death in November 2019. Nicholas Purnell QC is head of Cloth Fair Chambers. This chapter was reviewed before publication by Susannah Cogman, a partner in Herbert Smith Freehills' corporate crime and investigations practice.

2 *Lennards Carrying Co v. Asiatic Petroleum* [1915] AC 705, *Bolton Engineering Co v. Graham* [1957] 1 QB 159 (per Denning LJ) and *R v. Andrews Weatherfoil* [1972] 56 Cr App R 31 CA.

3 *Tesco Supermarkets Ltd v. Nattrass* [1972] AC 153.

4 *Meridian Global Funds Management Asia Ltd v. Securities Commission* [1995] 2 AC 500 PC.

of their employees. This difference in the probability of a successful prosecution explains, in part, why settlement agreements are far more prevalent in the United States than in the United Kingdom.

The statutory landscape in the United Kingdom is changing to make the prosecution of corporates easier for authorities. Section 7 of the Bribery Act 2010 created criminal liability for corporates who fail to prevent 'associated persons' (potentially including agents, subsidiaries and other third parties as well as employees) from committing bribery. The Criminal Finances Act 2017 includes a similar offence of failure to prevent the facilitation of tax evasion. Under this offence (which came into force on 30 September 2017) prosecutors will need to prove that tax evasion has occurred, that a person facilitated this evasion and that the facilitator was a person associated with the accused corporate. This type of offence of 'failure to prevent' may become increasingly common. The former Director of the Serious Fraud Office (SFO), Sir David Green QC, called on a number of occasions for the failure-to-prevent offence to apply to all financial and economic crimes and in early 2017 the Ministry of Justice called for evidence in relation to the introduction of such an offence. The current Director of the SFO, Lisa Osofsky, has also advocated for such an extension, although her preference would be to replace the identification principle for corporate criminal liability with a vicarious liability model.[5] In March 2019, the UK Parliament's Treasury Select Committee published a report following its economic crime inquiry,[6] which included suggestions received from the SFO either to replace the identification principle with a form of vicarious liability[7] or to introduce a new offence of failing to prevent economic crime. The committee made no recommendation as to which suggestion it preferred but appears to have favoured extending the failure-to-prevent offence.[8] On 7 May 2019, the government published its response to the Treasury Select Committee's report, stating that its analysis of the responses to the call for evidence was concluded and that the Ministry of Justice will respond 'shortly'.[9] The heightened threat of a successful prosecution, which would result from the introduction of a broad failure-to-prevent offence for all financial and economic crimes, may in turn lead to an increase in the prevalence of settlements of criminal proceedings in England and Wales.

Each option for settlement currently available to a corporate has its own particular advantages and disadvantages, but a common feature is that they are all

5 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/serious-fraud-office/oral/94785.pdf; https://www.lawgazette.co.uk/law/parliament-urged-to-create-all-encompassing-failure-to-prevent-law/5068369.article.

6 https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/news-parliament-2017/report-published-economic-crime-17-19/.

7 The SFO's proposal was that a company would be guilty of an offence if a person associated with it commits the relevant offence intending to obtain or retain business for the company; to obtain or retain a business advantage for the company; or otherwise to benefit the company (financially).

8 See comments made by a specialist legal adviser to the committee, https://www.lawgazette.co.uk/peers-call-for-speedier-bribery-investigations-/5069588.article.

9 https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/2187/2187.pdf.

jurisdictionally limited in their effect to the United Kingdom. Where there are multiple investigating authorities, settlement negotiations in the United Kingdom will typically be approached as part of a larger, overarching strategy to settle current and prospective proceedings globally.

UK authorities are increasingly participating in global settlements, particularly with their US counterparts. It may yet be too early to identify any trends, although one distinct feature has emerged: the central role of the UK judiciary. The *Innospec* settlement was criticised by the senior judge who heard the case, Lord Justice Thomas, for being presented as a 'done deal',[10] and the DPA model introduced in the United Kingdom departs significantly from its US counterpart by being conditional on substantial judicial review and approval.[11]

Until the cases of *SFO v. Sarclad Limited*[12] and *SFO v. Rolls-Royce PLC and Rolls-Royce Energy Systems Inc*,[13] a further feature of settlements concluded by the UK authorities appeared to be that they were more likely to be successful if the criminal conduct had been contained to an isolated incident. For example, the Balfour Beatty plc settlement (which resulted in the first CRO against a corporate in the United Kingdom) related to one particular contract.[14] The first DPA in the United Kingdom, involving Standard Bank plc (now ICBC Standard Bank plc (Standard Bank)), concerned a particular debt transaction.[15] *XYZ Ltd (Sarclad)* involved an SME that generated the majority of its revenue via sales to Asian markets, through the systematic offer and payment of bribes to secure contracts in a number of foreign jurisdictions over the course of roughly eight years.[16] This conduct could not be said to be contained, involving as it did at least 28 separate contracts, although the misconduct was alleged to have been carried out by a small number of employees. *Rolls-Royce* involved corruption across multiple business lines in seven jurisdictions over the course of 24 years with the involvement of senior management, described in the judgment as 'egregious criminality' involving 'truly vast corrupt payments'.[17] Whether *Rolls-Royce* is the high-watermark of criminality in corporate settlements remains to be seen, but the trend in these cases suggests that isolated or contained criminality may no longer be a prerequisite for securing a settlement with UK authorities.

10 *R v. Innospec Ltd* [2010] 3 WLUK 784, [2010] Lloyd's Rep FC 462, [2010] Crim LR 665, at paras. 26 to 29 (*Innospec*).

11 Section 45 and Paragraph 7, Schedule 17, Crime and Courts Act 2013 (UK).

12 *Serious Fraud Office v. XYZ Ltd* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509; the company in this case was originally anonymised as 'XYZ' to avoid prejudicing criminal proceedings against individuals arising out of the same facts. Following the acquittals of the individuals, the company was identified.

13 *SFO v. Rolls-Royce PLC and Rolls-Royce Energy Systems Inc* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249 (*Rolls-Royce*).

14 'Balfour Beatty plc', press release dated 6 October 2008, SFO.

15 *SFO v. Standard Bank plc (now ICBC Standard Bank Plc)* (Case No. U20150854) [2015] 11 WLUK 804, [2016] Lloyd's Rep FC 102 (*Standard Bank plc)*.

16 *Serious Fraud Office v. XYZ Ltd* (Case No. U20150856) [2016] 7 WLUK 211, [2016] Lloyd's Rep FC 517 at paras. 6, 7.

17 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249, at para. 61.

Corporates facing proceedings in more than one jurisdiction could seek to settle each set of proceedings individually, but the idea behind a global settlement is to coordinate these negotiations. In theory, a global settlement should be a 'win-win' scenario for both the corporate and the investigating authorities. By acting in concert, the investigating authorities are able to exert more pressure on the corporate to settle than they each are likely to have been able to do in isolation. For the corporate, a global settlement is potentially a fairer outcome as the penalty will be assessed holistically. A global settlement also achieves more finality than a domestic prosecution, which confers only limited double jeopardy protection (in those jurisdictions where such protection is granted). As in *Standard Bank*, in *Rolls-Royce*, the corporate was required under the terms of the DPA to assist law enforcement agencies, regulators and multilateral development banks, including those overseas, at the reasonable request of the SFO. It was also recognised in the judgment that there remained a risk that Rolls-Royce would face liability in jurisdictions not covered by the global settlement involving the United Kingdom, the United States and Brazil.[18]

In practice, global settlements can involve significant risks. A recent example is the prosecution in Greece of former employees of Johnson & Johnson and its subsidiary, DePuy International Limited (DePuy), which included the prosecution of one individual, Robert Dougall, notwithstanding his 2010 prosecution by the SFO and conviction and sentence.[19] Although Dougall was acquitted in the Greek proceedings, this case demonstrates that no settlement can confer an absolute guarantee against further proceedings in any jurisdiction – particularly not in jurisdictions where there is no limitation period for criminal offences (as in the United Kingdom, other than for summary offences). Dougall's prosecution must be contrasted with the outcome of the SFO's investigation of DePuy. The company was investigated by the SFO following a referral from the United States Department of Justice (DOJ), which, along with other domestic and foreign authorities, had been investigating Johnson & Johnson in relation to payments made by DePuy to intermediaries for the purpose of making corrupt payments to Greek medical professionals working in the Greek public health system.[20] The DOJ concluded a DPA with Johnson & Johnson in the United States as part of a global settlement over the unlawful conduct in Greece.

The SFO sought a CRO against DePuy rather than pursuing any criminal prosecution on the basis that such prosecution was prevented in the United Kingdom by the principle of double jeopardy. The former Director of the SFO, Sir David Green QC, had taken the view that the underlying purpose of the rule against double jeopardy is to stop a defendant from being prosecuted twice for the same offence in different jurisdictions: Johnson & Johnson's DPA with the DOJ had the legal character of a formally concluded prosecution and punished

18 Ibid. at para. 68.

19 *R v. Dougall* [2010] EWCA Crim 1048 (*Dougall*).

20 'DePuy International Limited ordered to pay £4.829 million in Civil Recovery Order', press release dated 8 April 2011, SFO.

the same conduct in Greece that had been investigated by the SFO. That double jeopardy will be a bar to prosecution where a defendant has been convicted or acquitted by a foreign court on the same facts is uncontroversial,[21] but whether the conclusion of a DPA in the United States is equivalent to a formally concluded prosecution has not been tested in the courts. The SFO gave no detailed argument as to why it concluded that DePuy's prosecution in the United Kingdom was barred, and the application of the principles of double jeopardy in global settlements remains unclear.[22] The SFO's reasoning in relation to DePuy will also be problematic where as part of a global settlement it is seeking to agree its own DPA in the United Kingdom following their introduction in 2014. If the SFO considers itself prevented by the rules of double jeopardy from pursuing criminal prosecution against a corporate that has agreed a DPA or other settlement with foreign authorities, then it may be prevented from agreeing a DPA under the statutory regime in the United Kingdom as prosecution may always follow a DPA if its terms are breached.[23]

Furthermore, no settlement can prevent private civil litigation, which could potentially be assisted or even encouraged by material generated in connection with the settled proceedings. However, settlement could make civil action less likely (or at least less likely to be successful), than were a contested criminal trial to take place, by reducing the volume of material entering into the public domain as compared to a full trial of the facts.

Whether a global settlement is worth pursuing is therefore likely to depend very much on the circumstances of each case. A key consideration will be the jurisdictions and agencies involved, and the particular form or forms of settlement contemplated.

23.2 Initial considerations

This chapter assumes that the corporate has already decided that a settlement is desirable in principle. This is not a straightforward exercise and will involve many of the considerations discussed in the other chapters in this book. This is likely to include a comparison of the cost involved of agreeing a settlement (and any agreed financial penalty) as against the cost involved of defending criminal proceedings and the probability of a conviction (and any penalty imposed). It will also include the reputational damage that contested criminal proceedings may have on a corporate. Corporates should also consider that a criminal conviction

21 *Treacy v. DPP* [1971] AC 537 *per* Lord Diplock; see also the Decision of the Grand Chamber of the European Court of Justice in *Kossowski* (C-486/14, 29 June 2016), setting out the court's views on double jeopardy and its operation across EU Member States.

22 See the issue discussed in more detail in 'Deterring and Punishing Corporate Bribery: An evaluation of UK corporate plea agreements and civil recovery in overseas bribery cases', Transparency International UK policy paper published in May 2012, at paras. 353 to 361.

23 Paragraph 9, Schedule 17, Crime and Courts Act 2013 (UK).

for certain economic and financial crimes may exclude them from competing for certain public contracts.[24]

Of course a corporate may also successfully argue that the authority should not institute any proceedings against it: prosecutors must be satisfied of the evidential basis of the prosecution as well as the public interest in prosecuting.[25] Many investigations in the United Kingdom result in no further action being taken against the subject of the investigation.

The attractiveness of a settlement is likely to vary considerably depending on the conduct under investigation and the investigating authorities involved. It is also likely to depend on the form of settlement available – for example, the advantages to a corporate of agreeing to a DPA in the United Kingdom are likely to be very far removed from the advantages of agreeing to a DPA in the United States. In some circumstances a settlement in the United Kingdom might not be an attractive prospect when considered in isolation, but the ability to secure a linked settlement with investigating authorities in another jurisdiction could tip the balance in favour of seeking a UK settlement as part of a global resolution.

Given that a settlement may not always be an obvious choice, the reasons for seeking to settle and the reasons for choosing a particular form of settlement should be clear before negotiations commence. The initial assessment of the corporate's eligibility for the kind of settlement sought must be realistic, based on the best available information about the conduct and a thorough understanding of the attitude and approach adopted by the relevant authorities. The corporate will also need to be clear about the risks that settlement negotiations entail. In the event that the negotiations break down, the corporate might find itself in a worse position than it would have been in had it not entered into the negotiations in the first place. Finally, to demonstrate compliance with fiduciary obligations it will also be important to ensure that any decision makers have no personal interest in the outcome of settlement negotiations, as they would have if they were exposed to individual liability in connection with the conduct under investigation. This may be particularly complex in relation to small corporates where any decision-makers face individual liability for criminal conduct while simultaneously attracting liability to the corporate by acting as the directing mind and will.

Options for seeking a settlement 23.2.1

Civil recovery orders 23.2.1.1

A corporate could seek to persuade an investigating authority to dispose of an investigation by initiating civil recovery proceedings rather than a prosecution. This decision is not subject to judicial approval, as the decision on whether to prosecute rests solely with the prosecutor.

24 Public Contracts Regulations 2015 (UK); Public Contracts Directive, 2014/24/EU.

25 Crown Prosecution Service Guidance on Corporate Prosecutions, https://www.cps.gov.uk/legal-guidance/corporate-prosecutions.

Civil recovery proceedings can be brought in the High Court by a number of UK enforcement agencies against property of a value in excess of £10,000 believed to have been obtained through unlawful conduct.[26] As a form of settling criminal proceedings a CRO has many features that could be helpful when a UK settlement is sought as one aspect of a global settlement. No prior UK conviction is required. The standard of proof is the civil one of the balance of probabilities. Judicial approval does not need to be sought before a claim can be brought, and the High Court's jurisdiction to make the order extends over assets located overseas; although it may in practice be tempered by the local law position on enforcement of orders that are not based on a conviction.

A CRO was for many years regarded as the best possible settlement outcome for corporates facing potential criminal proceedings in the United Kingdom, and an outcome that could plausibly be expected in a corporate self-reporting case. Two developments have impacted on this view.

First, under its current policy, the SFO will be less ready than it historically has been to dispose of an investigation by way of a CRO.[27] In part, this is a response to the OECD's criticisms of the UK's lack of commitment to combating bribery of foreign public officials.[28] In the event that the SFO were to agree to a CRO, its terms will now be published in full, which removes some of the historically perceived benefit of this form of settlement.[29]

Secondly, the SFO has demonstrated that civil recovery proceedings and criminal proceedings are not necessarily mutually exclusive provided that the conduct can be divided. In conjunction with the conviction of Bruce Hall in 2012 and the making of a confiscation order and compensation order against him, the SFO brought civil recovery proceedings in respect of conduct falling outside the scope of the indictment because UK jurisdiction did not arise.[30] This has to be considered, however, against the background of the criticism by Thomas LJ in *Innospec* of the use of a CRO in addition to trial on indictment; Thomas LJ concluded that where the facts and public interest determined that a prosecution was appropriate, the use of the civil jurisdiction was consequently inappropriate. In particular, the

26 Part V, Proceeds of Crime Act 2002 (UK) (POCA). Section 316 of POCA defines 'enforcement authority' in England and Wales as the National Crime Agency, the Director of Public Prosecutions or the Director of the SFO. The financial threshold of £10,000 is set in section 287, POCA and the Proceeds of Crime Act 2002 (Financial Threshold for Civil Recovery) Order 2003 (UK).

27 Guidance on Corporate self-reporting, issued by the SFO, revised in October 2012. Note also the position in Scotland where the Crown Office and Procurator Fiscal Service issued guidance in June 2017 stating that prosecutors may consider civil settlement for corporates that self-report offences under the Bribery Act 2010.

28 'Report on the Application of the Convention on Combating of Foreign Public Officials in International Business Transactions and the 1997 Recommendations on Combating Bribery in International Business Transactions', approved and adopted by the OECD Working Group on Bribery in International Business Transactions on 16 October 2008.

29 Statement of David Green QC, then Director of the SFO, 17 April 2013. See, e.g., 'Oxford Publishing Ltd to pay almost £1.9 million as settlement after admitting unlawful conduct in its East African operations', press release dated 3 July 2012, SFO.

30 'Bruce Hall sentenced to 16 months in prison', press release dated 22 July 2014, SFO.

judge deprecated the possibility of matters arising in the same case coming within the jurisdiction of two separate judges from two separate courts. In contrast, the use of a CRO for DePuy was less problematic as the corporate was not the subject of an indictment.

See Section 23.1

Deferred prosecution agreements 23.2.1.2

A DPA may be regarded as the half-way house between a negotiated plea agreement and a CRO. It remains to be seen whether it will be a popular form of settlement or whether it will be confined to isolated instances. First, a DPA is only available in limited circumstances. Secondly, the power to apply to the courts for a DPA rests solely with the prosecutor,[31] and the DPA provisions reserve to the prosecutor (currently only the SFO or the Crown Prosecution Service (CPS)) the right to extend any invitation to enter into DPA negotiations. Thirdly, as was identified by the former Director of the SFO,[32] the high threshold for corporate criminal liability under English law reduces the incentive for corporates to enter into a DPA at all. To date, all five DPAs secured in the United Kingdom have not faced any difficult application of corporate criminal liability: *Standard Bank plc* related to the strict liability offence of failing to prevent bribery under section 7 of the Bribery Act 2010; *XYZ Ltd (Sarclad)* applied to a small company in which the directing mind and will was easily identified; *Rolls-Royce* related to the strict liability offence of failing to prevent bribery as well as substantive offences of bribery and corruption involving, on the facts as admitted by Rolls-Royce for the purposes of the DPA, controlling minds of the company; and in *Tesco Stores Limited*[33] and *Serco Geografix Limited,*[34] the alleged offences were said to have been committed by a number of senior individuals who the parties accepted constituted the directing mind and will of the respective companies. Experience will demonstrate to what extent a corporate entity can introduce the possibility of a DPA into any discussions it may hold with the SFO.[35]

In theory, a DPA should be an attractive form of settlement as the corporate is never actually prosecuted, avoiding some of the stigma and adverse publicity necessarily associated with a criminal trial and a conviction. A corporate will have the opportunity to make representations on and to influence the terms of the settlement that is made public, and there will be no mandatory debarment from public contracts. Importantly, a DPA may be part of a global resolution that may be in the overall commercial interests of the corporate.

The corporate is nevertheless the subject of criminal proceedings that are suspended. The offences alleged to have been committed are particularised in an

31 See Paragraph 8, Schedule 17, Crime and Courts Act 2013 (UK).

32 Sir David Green QC, then Director of the SFO, speech given at Pinsent Masons and Legal Week Regulatory Reform and Enforcement Conference, 24 October 2013.

33 *SFO v. Tesco Stores Limited* (Case No. U20170287) [2017] 4 WLUK 558.

34 *SFO v. Serco Geografix Limited* [2019] 7 WLUK 45 (*Serco Geografix Limited*).

35 Deferred Prosecution Agreement Code of Practice, issued by the Director of Public Prosecutions and Director of the SFO (DPA Code of Practice), at para. 2.1.

indictment, and further detailed in the statement of facts accompanying the DPA. The terms of the DPA will include not only a penalty intended to reflect the penalty that would have been imposed on a guilty plea but also disgorgement of profits and potentially compensation payments. Unlike a criminal sentence, a DPA may extend to requiring the corporate to submit to a compliance monitor for a specified period.[36]

The terms of the DPA may require the corporate to disgorge the gross profit made as a result of the criminal conduct.[37] The DPA may also impose a financial penalty,[38] which must be broadly comparable to the fine that a court would have imposed on conviction and is accordingly assessed by reference to the relevant Sentencing Guideline for fraud, bribery and money laundering offences (Sentencing Guideline).[39] Where the corporate has limited means and ability to meet these financial obligations, the court may nevertheless approve a penalty that would render the corporate insolvent where it would be in the interests of justice to do so.[40] Among other things, the court will consider the impact of any financial penalty on the corporate's staff, service users, customers and the local economy. In *XYZ Ltd (Sarclad)*, the corporate's parent agreed to provide financial support to Sarclad by returning almost £2 million from dividends received for Sarclad to pay towards disgorgement.[41] The court made clear that the innocent parent was under no contractual or legal obligation to contribute towards the financial penalty imposed on its subsidiary for the criminal conduct.[42] However, the court did point out that the parent had received £6 million in dividend payments since acquiring Sarclad.

In *Rolls-Royce*, the total financial orders (including those imposed in the United States and Brazil) amounted to over £650 million even after a 50 per cent reduction to the UK element of the financial penalty in recognition of Rolls-Royce's 'extraordinary' co-operation.[43] The Court was satisfied that this figure was sufficient to bring home to both management and shareholders the need to operate within the law without being so high as to put Rolls-Royce out of business, which would have been inappropriate in the circumstances.[44]

In *Serco Geografix Limited*, the company was ordered to pay a financial penalty of £19.2 million and the SFO's investigative costs of £3,723,679. The company would also have been required to pay compensation of £12.8 million, but this was

36 Schedule 17, Crime and Courts Act 2013 (UK).

37 Paragraph 5(3)(d), Schedule 17, Crime and Courts Act 2013 (UK).

38 Paragraph 5(3)(a), Schedule 17, Crime and Courts Act 2013 (UK).

39 Fraud, bribery and money laundering offences: Definitive guideline, issued by the Sentencing Council, in force from 1 October 2014.

40 *Serious Fraud Office v. XYZ Ltd* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509 at paras. 23, 24.

41 Ibid. at para. 22.

42 Ibid. at para. 21.

43 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249 at para. 128.

44 Ibid. at para. 127.

fully offset by payments made pursuant to Serco Limited's 2013 settlement agreement with the UK Ministry of Justice.[45]

The process of negotiating a DPA could itself deter a corporate from seeking this sort of settlement. It is lengthy and uncertain, as any agreement reached with the relevant prosecuting authority is ultimately conditional on judicial approval. It is accompanied by potentially as great a degree of public scrutiny as may be attracted by contested criminal proceedings. The provision of false, misleading or incomplete information to the relevant prosecuting authority could amount to an offence,[46] and it can be extremely challenging for a corporate, and the relevant individual within the management structure, to certify that the material provided to the investigating agency is complete.

The DPA may become a more attractive option for corporates if there is more flexibility on the terms imposed and if higher discounts to financial penalties or sentences continue to be applied. With respect to increased discounts, the DOJ's enhancements to its Pilot Program could be of interest to the SFO. In November 2017, the DOJ announced that the Pilot Program it launched in 2016 to encourage companies to self-report potential violations of the Foreign Corrupt Practices Act (FCPA) would be made permanent and incorporated into the United States Attorneys' Manual (now known as the Justice Manual), subject to some amendments.[47] Under the revised FCPA Corporate Enforcement Policy, where a company 'satisfies' the DOJ's standards of self-reporting, co-operating and remediating, there will be a 'presumption' that the government will resolve the matter with a declination – unless there are aggravating circumstances (for example, recidivism). However, even where circumstances 'compel' an enforcement action, the DOJ will recommend a 50 per cent reduction off the low end of the Sentencing Guideline fine range for self-reporting companies.

In the DPA reached with Sarclad, the court stated that a discount of 50 per cent to the financial penalty that would have been imposed[48] was appropriate, given that the corporate had self-reported and admitted the criminal conduct far in advance of the earliest possible opportunity that would have applied after a criminal charge.[49] This sizeable reduction was not based on an application of the Sentencing Guideline or the DPA statutory provisions themselves.

45 *Serco Geografix Limited* [2019] 7 WLUK 45 at para. 37.

46 For example, for attempting to pervert the course of justice, contrary to the common law. Prosecution of the offence that is the subject of the DPA can also follow if the organisation provided information to the SFO that it knew or ought to have known was inaccurate, misleading or incomplete, see *XYZ Ltd (Sarclad)* and *Rolls-Royce*.

47 'Deputy Attorney General Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices Act' Press release, 29 November 2017.

48 In fact, as the judge made clear, the question of a penalty was 'academic because, given the amount disgorged, whatever multiplier is chosen and however substantial the discounts, the result is a figure which Sarclad simply cannot pay and which would result in its insolvency.', at para. 55.

49 *Serious Fraud Office v. XYZ Ltd* (Case No. U20150856) [2016] 7 WLUK 211, [2016] Lloyd's Rep FC 517.

Even more surprising (at first glance) was the application of a 50 per cent discount to the financial penalty in *Rolls-Royce*, where the corporate did not make the initial self-report.[50] The initial report of suspicions of criminality in the corporate's civil business in Asia came from public internet postings and precipitated the SFO's investigation; however, this led to an immediate and extensive investigation by the corporate during which it made a number of voluntary reports to the SFO in respect of other business lines in multiple jurisdictions.[51] Rolls-Royce's co-operation with the SFO and other authorities was said to be 'extraordinary'.[52] Rolls-Royce took a number of steps in addition to the extensive investigation and voluntary reports to authorities: it reviewed relationships with intermediaries, agents, advisers and consultants; provided over 30 million documents in electronic and hard copy form (Rolls-Royce agreed to the use of digital methods to identify privilege issues in the material and the use of independent counsel in relation to the privilege review); allowed the SFO to interview witnesses first and waived privilege over its own internal interview memoranda; provided material to the SFO voluntarily (without need for recourse to compulsory powers); consulted with the SFO in respect of media coverage; provided all financial data sought by the SFO and co-operated with financial assessments undertaken; and sought the SFO's permission before winding up companies that may have been implicated in the SFO's investigation.

The SFO submitted that in the particular circumstances of the case, the Court should not distinguish between the corporate's assistance and that of those who have self-reported from the outset. This was accepted on the basis that what Rolls-Royce reported was far more extensive and of a different order than might have been exposed without its co-operation.[53] The Court was satisfied that, from the moment of the initial question from the SFO prompted by the public postings on the internet, Rolls-Royce could not have done more to expose its own misconduct. Self-reporting was said in the judgment to be a core purpose of DPAs, and the weight this attracts depends on the totality of the information provided; it seems that the measures that Rolls-Royce took to unearth and report the extent of the criminality made up for the absence of an initial self-report.[54]

The decision in *Serco Geografix Limited* revisited the issue of self-reporting and co-operation. In his concluding comments, Mr Justice Davis noted that any cynicism about the process by which a corporate entity can take advantage of a DPA 'is not well-founded' and that approval will only be given where there is the 'clearest possible demonstration of integrity' on the part of the relevant company, which will require self-reporting, full co-operation with the investigation, a willingness to learn lessons and acceptance of an appropriate penalty. He added that a willingness to learn lessons must be shown via 'real, substantial and continuing

50 *Rolls-Royce* (Case No. U20170036) [2017] [2017] 1 WLUK 189, Lloyd's Rep FC 249 at para. 123.

51 Ibid. at para. 17.

52 Ibid. at paras. 16 to 20 and 121.

53 Ibid. at para. 22.

54 Ibid. at para. 38.

remedial measures'.[55] The court proceeded to apply a 50 per cent discount and referred to the fact that in all but one of the earlier instances of approval of DPAs, the financial penalty has been discounted by 50 per cent rather than one third. This was found to 'encourage corporate responsibility in terms of early reporting of criminal conduct'.[56]

There is a clear view among practitioners that the incentives to enter into a DPA, in particular the apparent maximum discount on penalty, embedded within the statutory scheme,[57] of one-third (the same as for an early guilty plea) is insufficient and fails to recognise the positive factors in the conduct of the corporate that will have led to the offer of a DPA in the first place. This view appears to have been accepted by the SFO and the judiciary, as a 50 per cent reduction has been applied on each occasion since the *Standard Bank plc* DPA.

Negotiated plea agreements 23.2.1.3

A plea agreement can be negotiated with the prosecutor at any stage after indictment, up to the conclusion of the trial. It may be preceded by advance representations on charge, which a prosecutor is under no obligation to consider but may do so at his or her discretion. Both advance representations and plea agreements could potentially reduce the scope of the conduct charged, or even determine the nature of the offence charged; as seen in *BAE Systems*,[58] where the corporate had been investigated for overseas corruption but pleaded guilty to knowingly procuring the failure of its subsidiary, British Aerospace Defence Systems Ltd (BADS), to comply with the provisions of section 221 of the Companies Act 1985, and thereby aiding and abetting, counselling and procuring the commission of the offence contrary to section 225 of the Companies Act, by the officers of BADS.[59] In *BAE Systems*, Mr Justice Bean was critical of the restriction on the scope of the conduct in the settlement reached between the corporate and the SFO, and in light of these criticisms prosecuting authorities may in future be less willing to minimise the conduct in negotiated plea agreements.[60] Mr Justice Bean made clear that in cases involving negotiated plea agreements the judge will not be bound by the agreement between the prosecution and the defence, and the prosecution's view on the proposed basis of the plea is deemed to be conditional on the judge's acceptance of the basis of the plea.[61] The judge made clear that the involvement of the criminal courts precludes the passing of a sentence on an artificial

55 *Serco Geografix Limited* [2019] 7 WLUK 45 at para. 47.

56 Ibid. at para. 37.

57 Schedule 17 Paragraph 5(4), Crown and Courts Act 2013 (UK).

58 *R v. BAE Systems plc* [2010] EW Misc 16 (CC) (*BAE Systems*).

59 *Corruption and Misuse of Public Office* (2nd Ed.), Collin Nichols QC, Timothy Daniel, Alan Bacarese and John Hatchard, at p. 39.

60 *BAE Systems* at para. 13.

61 *R v. Underwood* [2004] EWCA Crim 2256; BAE Systems at para. 13.

basis. While Mr Justice Bean accepted the basis of the sentence in *BAE Systems*, this may not always be the case.[62]

The judge also expressed surprise that the SFO had committed to a blanket indemnity against investigations or prosecutions of any member of the BAE Systems group for past conduct whether disclosed or otherwise.[63]

However, even if the charges remain unchanged, a guilty plea at the earliest possible stage makes the corporate eligible for a reduction of up to one-third off the sentence that would otherwise have been imposed on conviction.[64]

UK prosecutors will always be open to negotiations on plea. The prosecution and the defence are in all cases required to resolve issues and agree evidence wherever possible prior to trial.[65] The prosecutor must, however, have regard to any applicable restraints on the exercise of discretion, including the Witness Charter and the Code of Practice for Victims of Crime.[66] In accordance with the Code for Crown Prosecutors, prosecutors will also need to ensure that the plea reflects the seriousness and extent of the offending.[67] The Attorney General's Guidelines to the legal profession state that prosecutors must not agree to a basis of plea that is misleading, untrue or illogical or insupportable.[68] Where a case involves multiple defendants, the bases of plea must be factually consistent. Trial judges may ultimately, of their own motion, disregard the agreement and direct a 'Newton' hearing to establish the relevant facts.[69]

Just as the decision on whether to accept a proposed basis of plea is ultimately one for the trial court, it is similarly for the sentencing court to impose the sentence on conviction. In cases of serious and complex fraud the Attorney General's Guidelines permit the prosecution and defence to present a joint written submission to the court on sentence but this is not binding on the court. In *Dougall*, the court declined to impose the SFO's suggested suspended sentence on an assisting offender, although the custodial sentence that the court did impose was overturned on appeal. The Court of Appeal criticised the SFO for adopting a role that was more akin to that of the defence. The courts in *BAE Systems* and in *Innospec* felt compelled to accept the suggested sentences because they formed part of a global settlement that the corporate entity had been invited to accept (and

62 The principles underlying this reasoning are also reflected in the statutory regime for DPAs, which must be approved by a judge as being in the interests of justice; see further Section 23.2.1.2.

63 *BAE Systems* at para. 5.

64 Reduction in Sentence for a Guilty Plea: Definitive guideline, Sentencing Council, 23 July 2007, at para. 4.2 (for cases where the first hearing was before 1 June 2017); Reduction in Sentence for a Guilty Plea: Definitive Guideline, Sentencing Council, 7 March 2017, para. D1 (for cases where the first hearing was after 1 June 2017).

65 Rule 3.3, Criminal Procedure Rules 2015 (UK).

66 The Witness Charter, issued by the Ministry of Justice, December 2013; Code of Practice for Victims of Crime, issued by the Ministry of Justice, October 2015, last updated 8 October 2018.

67 The Code for Crown Prosecutors, October 2018, at para. 9.

68 See 'Plea discussions in cases of serious or complex fraud', 29 November 2012; and 'The acceptance of pleas and the prosecutor's role in the sentencing exercise', 30 November 2012, Attorney General's Office.

69 Consolidated Criminal Practice Direction, at para. IV.45.10.

because of the corporate's limited financial resources in *Innospec*), but Thomas LJ in *Innospec* warned that this approach would not be repeated in the future.

The attractiveness of a plea agreement to a corporate will depend largely on the weight of the prosecution evidence, including the existence of any co-operating co-offenders under the 'offender assistance' provisions set out in sections 71 to 75 of the Serious Organised Crime and Police Act 2005. In particular, the corporate's willingness to plead is likely to reflect an assessment that the prosecutor would be able to establish corporate criminal liability. As mentioned in the introduction to this chapter, guilty pleas by corporates are more likely to be forthcoming for offences where the identification principle does not apply or liability is strict, or both, or where the corporate is small and lines of responsibility are clear; by contrast, the prosecution might in other cases struggle to identify culpable senior management.

The size of the likely penalty will also be a factor when the corporate is considering whether to plead. There is an established procedure in place by which a defendant in Crown Court proceedings can seek a binding indication from the trial judge of what sentence would be imposed on a guilty plea (*Goodyear* indication).[70] That Guideline may have similarly increased the attractiveness of plea agreements for corporates, not only by making the likely sentence more predictable at an even earlier (pretrial) stage but also by increasing the risk of higher penalties being imposed than has historically been the case and thereby incentivising an early, negotiated settlement.

The downsides of a plea agreement include the inability to contest the charges in a public forum, and loss of the opportunity of an acquittal. The advantages of a plea agreement also decline rapidly with time once a trial is under way.

There are also risks arising from plea negotiations. The Attorney General's Guidelines state that the prosecutor may not rely on the defendant's participation in plea negotiations or on any information disclosed during those negotiations as evidence against the defendant in the event that the negotiations fail but a signed plea agreement can be relied on as confession evidence against the defendant. A prosecutor would normally be free to rely on any evidence gathered as a result of enquiries made on the back of information disclosed in the course of the negotiations, and information provided by the defendant in connection with the negotiations could normally be relied on both in related prosecutions of other defendants and in a prosecution of the defendant for another offence. In addition, the prosecutor might be obliged to disclose material relevant to the negotiations to a co-defendant.

70 In accordance with *R v. Goodyear* [2005] EWCA Crim 888 and by reference to the Sentencing Guideline.

23.2.2 Strategic considerations when seeking a settlement in the United Kingdom

Once a corporate has decided in principle to seek to settle criminal proceedings in the United Kingdom, the objective will be to achieve the desired form of settlement as effectively as possible, avoiding or minimising, to the extent possible, adverse consequences. This section will discuss common strategic considerations that are likely to arise at the outset and during the early stages of settlement negotiations.

23.2.2.1 Timing of settlement

A preliminary strategic consideration will be the point at which to approach the relevant authority. On the one hand, a successful outcome is more likely the earlier an approach is made. The financial and reputational costs to a corporate of being a subject of a criminal investigation and prosecution will increase incrementally and early self-reporting is an important factor in determining whether a DPA will be offered. Clearly, however, the corporate needs to have sufficient knowledge about the conduct it proposes to report.

A corporate may self-report the conduct in question or otherwise bring it to the attention of relevant authorities, for example, pursuant to money laundering reporting obligations or, for listed corporations, obligations to disclose information to the market. The SFO had published guidance on self-reporting in 2012[71] and has recently published internal guidance outlining what it considers to be good practice with respect to co-operation by a company under investigation.[72]

In all other cases the determining factor is likely to be the type of settlement sought. Where the favoured outcome is a CRO, the driver will be to reach agreement on this form of alternative disposal before any steps are taken to initiate criminal proceedings. If the preferred form of settlement is a DPA, the timing of the settlement will be dictated by the DPA Code of Practice, but again will involve negotiations with the authority before the commencement of criminal proceedings. A settlement could be reached at any of the following points in time.

See Section 23.2.1.2

Before major production of documents

A corporate must balance the need to understand any potential criminal liability it faces with the benefit of making an early report to an authority. As stated above, corporates should establish sufficient knowledge of the circumstances before deciding to seek a settlement. Once that decision has been made, it is unlikely that an agency in the United Kingdom will be prepared to reach a settlement agreement without receiving all relevant documentation and undertaking some form of investigation. Once in the hands of the authorities, any material provided could be used against the corporate and individuals. In addition, such

71 Guidance on Corporate self-reporting, issued by the SFO, revised in October 2012. See also the Guidance on corporate prosecutions issued by the Director of Public Prosecutions, the Director of the SFO and the Director of the Revenue and Customs Prosecutions Office, issued in 2009/2010.

72 Corporate Co-operation Guidance, issued by the SFO, on 6 August 2019.

material can be provided to other domestic and international agencies and may ultimately be disclosed in any related civil proceedings. It has to be assumed that documents provided to investigating agencies may ultimately end up in the public domain.

Before witness testimony

To the extent that corporates record any interviews they conduct, UK authorities are likely to want access to these first accounts, which may raise issues of legal professional privilege. The Court of Appeal's judgment in *Director of the SFO v. ENRC*[73] has brought some much-needed clarity to this area of the law, following two conflicting first-instance decisions of the English High Court.[74]

The Court of Appeal in *ENRC* disagreed with the High Court's strict approach to whether notes of interviews attract litigation privilege. The High Court had concluded that only a prosecution, and not an investigation, amounts to 'litigation' and that 'contemplation' of a criminal investigation does not necessarily equate to the contemplation of prosecution, such that the first limb of the test for litigation privilege would be satisfied (namely that litigation is in progress or in reasonable contemplation). However, the Court of Appeal disagreed with this analysis, finding that uncertainty over whether criminal proceedings were likely would not in itself prevent litigation from being in reasonable contemplation, and that the whole subtext of the relationship between the relevant company and the authorities was important. In this case, the court found that the relationship between ENRC and the SFO meant that there was a possibility, if not a likelihood, of prosecution if the self-reporting process did not result in a settlement. The court also said that where the SFO made explicitly clear in its communications to the company that there was the prospect of a criminal prosecution, and external legal advisers were engaged to deal with that possibility, there was a clear ground for contending that criminal prosecution, and therefore litigation, was in reasonable contemplation at the time the interview notes were prepared.

The Court of Appeal also disagreed with the High Court's restrictive position on whether notes of interviews were prepared for the dominant purpose of litigation, which is the second limb of the test for litigation privilege. It found that the need to investigate the existence of alleged corruption was a subset of defending the litigation, and hence that notes made in interviews during the investigation stage were made for the dominant purpose of litigation.

This decision underlines the importance of obtaining advice when corporates need to conduct and create records of interviews during the fact-finding stage of an investigation, and before a prosecution decision is made by the authorities, to understand the alleged facts and any potential liability. Ordinarily, the SFO will still conduct interviews as part of its investigations following a self-report, even where there have already been interviews by the corporate. Nevertheless, the

73 *Director of the SFO v. ENRC* [2018] EWCA Civ 2006.

74 *Director of the SFO v. ENRC* [2017] EWHC 1017 (QB) and *Bilta (UK) Ltd & Ors. v. Royal Bank of Scotland and Mercuria Energy Europe Trading Ltd* [2017] EWHC 3535 (Ch.).

authorities may in some cases expect a corporate that wishes to obtain credit for co-operating, to waive privilege over certain documents that have been prepared during the investigation stage for the dominant purpose of engaging in settlement negotiations with the authorities. The SFO's recently published internal guidance on corporate co-operation[75] states that in addition to witness accounts, companies seeking credit for co-operating should provide any recording, notes and transcripts of interviews and identify a witness competent to speak to the contents of each interview. Legal advice on the limitations that should be explicitly placed on any privilege waiver a corporate proposes to provide is an essential safeguard.

Before indictment

In most cases, corporates will be seeking to settle before indictment. As discussed above, settlement negotiations may provide an opportunity to influence the content and timing of the indictment.

Before trial

A settlement at the early stages of criminal proceedings may help to mitigate reputational damage by reducing the amount of material made available to the authorities and, through them, potentially becoming available in the public domain or to other overseas agencies.

There may yet be benefits of settling after the commencement of trial. Although disclosure obligations will have been complied with and material may have been referred to in open court (thereby becoming accessible to the public), by avoiding witness testimony the corporate may minimise the risk of further reputational and other costs as a result of adverse prosecution testimony or unpredictable defence witnesses. Settling before conviction could potentially also serve a public relations objective in presenting the corporate publicly as being somewhat co-operative (despite initially contesting the proceedings).

23.2.2.2 Ability to secure a global settlement

An early settlement of UK criminal proceedings may also increase the prospects of concluding a global settlement. In the global settlement scenario, timing is likely to be primarily driven by the authority 'leading' the settlement negotiations. As press reports suggested in relation to the LIBOR investigation, there can be a 'race' among investigating authorities to charge defendants as a means of securing jurisdiction.[76]

Where a number of authorities may be investigating or have an interest in investigating the conduct, the potential for conflicts of jurisdiction to arise should be addressed by communications between prosecutors pursuant to multilateral

75 Corporate Co-operation Guidance, issued by the SFO, on 6 August 2019.

76 See, e.g., 'US DoJ issues arrest warrant for Briton in Libor probe', Caroline Binham, 6 February 2015, *Financial Times*.

and bilateral agreements such as the Eurojust guidelines for deciding which jurisdiction should prosecute and the Agreement for Handling Criminal Cases with Concurrent Jurisdiction between the United Kingdom and the United States.[77] Prosecutors engaged in plea negotiations in serious and complex fraud cases are directed by the Attorney General's Guidelines to liaise with any counterparts known to have an interest in the defendant, in accordance with the Prosecutors' Convention and any other relevant agreement or guidance.[78] However, these arrangements would not be enforceable by corporates who find themselves adversely affected by any departures from their terms; in any event, such agreements do not tend to address settlements.

In practice, constructive global settlement discussions require a high level of communication between the investigating agencies involved and also between the lawyers acting for the corporate and those investigating agencies. By way of example, in *Standard Bank plc* there was clearly a high level of communication between the SFO and the US DOJ (as well as between the bank's lawyers and both the SFO and the DOJ), which ultimately resulted in the DOJ confirming in writing in advance of the UK settlement that in view of the terms of the proposed settlement it did not propose to continue its own investigation.

The SEC, on the other hand, decided to continue with its own investigation into the civil (as opposed to criminal) consequences of the alleged conduct, which resulted in a separate settlement with the bank. Although the SEC's investigation related to separate issues, the bank completed its settlement with the SEC very shortly before the final DPA hearing in the United Kingdom and the settlement was announced on the same day. Coordinating the timing of the settlement so that it was announced at the same time was clearly in the bank's interests, as it ensured that the UK and US investigations into the conduct were resolved simultaneously, with the bank able then to draw a line under the events and focus on the future.

Similarly, in *Rolls-Royce* it was clear that substantial discussions had taken place between the SFO, the US DOJ and the Brazilian public prosecutor to ensure a coordinated global resolution of the relevant conduct; indeed, its DPA with the US DOJ was fully disclosed in the UK DPA proceedings,[79] and the DPA hearing in the United Kingdom was brought forward for reasons linked to the change in administration in the United States in January 2017.[80] Rolls-Royce announced settlements with those authorities in parallel with its DPA with the SFO. The corporate was apparently able to coordinate between prosecuting authorities such that it was prosecuted for different conduct in different jurisdictions;[81] it was also

77 Annex A – Eurojust Guidelines – 'Which Jurisdiction Should Prosecute?', Annual Report 2003, issued by Eurojust (revised in 2016); Agreement for Handling Criminal Cases with Concurrent Jurisdiction between the United Kingdom and the United States of America, January 2007.

78 Prosecutors' Convention 2009, agreed by a number of UK prosecuting authorities including, *inter alia*, the SFO, the FCA, the Crown Prosecution Service and the Attorney General's Office.

79 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249 at para. 5.

80 Ibid. at paras. 10 and 12.

81 Ibid. 17 January 2017 at para. 5.

given US$25 million credit by the DOJ for fines paid in Brazil in relation to conduct that was overlapping between its DPA in the United States and its leniency agreement in Brazil.[82]

It is important to keep in mind when negotiating simultaneous settlements with multiple authorities and regulators (both at home and abroad) that the subject ensures that the published findings in each investigation concluded by a negotiated settlement are consistent, as authorities may have an incomplete understanding, or different interpretation, of the facts.

23.2.3 Written submissions to UK prosecuting authorities

One important risk that settlement negotiations pose for corporates is that the material generated will be relied on in the event that the negotiations break down; whether by the recipient authority or by third parties. Even if settlement negotiations will attract confidentiality to varying degrees, there will always be a number of avenues through which material provided to the authorities may be made available to other authorities and to third parties.

The extent to which settlement negotiations will generate material, and the extent to which such material may be protected from onwards disclosure, will depend on the form of settlement in question. Written submissions made to a prosecutor in the course of negotiating a plea agreement are confidential and will only be made available to third parties where it can be shown that the prosecutor's obligation to preserve confidentiality is outweighed by a countervailing interest.[83] In DPA negotiations, both the form and content of documents are governed by statute and are not negotiable. These documents will include the draft statement of facts and the terms of the proposed DPA, as well as the preliminary application to the court.[84] The prosecutor will require these documents to be agreed before the application to the court can proceed. They will also include any submissions contained in related correspondence with the prosecutor, as well as minutes of any meetings between the corporate and the prosecuting authority.

23.2.4 Oral presentations to UK prosecuting authorities

Presenting information orally, as an alternative to written submissions, could in theory reduce the risk that settlement negotiations pose for corporates by limiting the amount of incriminating documentary material generated in settlement negotiations or otherwise provided to the authorities. As a strategy it is obviously conditional on securing the agreement of the prosecuting authority, and is not as frequently encountered in the United Kingdom as in the United States; but the SFO is known to have acceded to requests of this nature on occasion. Notably, this

82 'Rolls-Royce plc Agrees to Pay $170 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act Case', press release dated 17 January 2017, United States Department of Justice.

83 Guidance to accompany the Attorney General's Guidelines on Plea Discussions in cases of Serious or Complex Fraud, issued by the Director of Public Prosecutions, the Director of the SFO and the Director of the Revenue and Customs Prosecutions Office, 24 May 2012.

84 Paragraph 5, Schedule 17, Crime and Courts Act 2013 (UK).

approach was employed in relation to the first and second DPAs entered into in the United Kingdom. However, in the recent Administrative Court case of *AL v. SFO*,[85] the court, in the context of a criminal trial of individuals following the corporate's[86] entry into a DPA, criticised the use of 'oral proffers' as 'highly artificial' and expressed its surprise that the SFO did not more robustly demand the written notes of interviews made during an internal investigation. The judgment is likely to cause the SFO to be cautious about relying on oral proffers in future investigations and instead to more robustly challenge broad claims to privilege; a senior SFO manager has stated[87] that this decision emphasised the danger for the SFO in not challenging excessively wide claims of privilege. However, given the less restrictive approach taken to legal professional privilege by the Court of Appeal in *ENRC*, there is likely to be a tension between the authorities' desire to challenge wide claims to privilege and demand written notes of interviews, and the Court of Appeal's decision that written interview notes made during an internal investigation are capable of being covered by litigation privilege. Therefore although oral proffers may no longer be acceptable, the authorities and co-operating corporates may find themselves in a predicament. The corporate should avoid inadvertent waivers of privilege, and the SFO is also unable to demand written interview notes made while litigation was reasonably in contemplation, and for the dominant purpose of litigation, as interpreted by the Court of Appeal in *ENRC*. In such cases, it is possible that the authorities may stress the importance of a corporate's co-operation in settlement discussions and therefore seek voluntary waivers of privilege over such documents by the corporate.

See Section 23.4

It also raises the prospect that, in multi-agency settlements, there might be a divergence of approach between agencies that are content to receive oral proffers (e.g., the US Department of Justice, which regularly accepts them) and those that are not. Oral summaries of privileged information and material could still be considered by the prosecuting authority as a limited (or indeed full) waiver of privilege, as there is no settled case law in the United Kingdom on this point, which could create a risk of collateral waiver of privilege in other jurisdictions or over other material. If the underlying interviews were not privileged, a prosecutor's notes from the presentation could potentially be disclosed to third parties, without the corporate having an opportunity to confirm whether the impressions recorded are correct.

See Section 23.2.2.1

An indication of the possible approach of courts in the United Kingdom can be gleaned from a ruling in proceedings against Dennis Kerrison and Miltiades Papachristos (employees of Innospec)[88] in which His Honour Judge Goymer considered whether a PowerPoint presentation to the SFO/DOJ that referred

85 [2018] EWHC 856.

86 Now known to be Sarclad Limited.

87 20 June 2018 speech given at Herbert Smith Freehills Annual Corporate Crime and Investigations Conference 2018, available at https://www.sfo.gov.uk/2018/06/21/corporate-criminal-liability-ai-and-dpas/.

88 13 May 2013 unreported.

to the notes of interviews conducted by the corporate with a prosecution witness amounted to a waiver of legal professional privilege in those interviews. The judge decided that there was not sufficient deployment of the interview notes in the PowerPoint presentation such as would amount to a collateral waiver of legal professional privilege in respect of those notes. It was conceded in argument that the PowerPoint presentation was subject to privilege, and as such there was no detailed discussion of the application of the principles of litigation privilege in this case. This is not always so in the investigations context, following *Three Rivers No. 5*.[89] The Court of Appeal has considered more recently the ambit of litigation privilege in one of the many cases relating to the SFO's investigation into the Tchenguiz brothers, stressing the importance of the 'dominant purpose' test.[90]

23.3 Legal considerations

Settlement negotiations should only be undertaken with a thorough understanding of the legal framework that governs the particular form of settlement pursued, and any relevant policies that govern the approach adopted by the relevant prosecuting authority. A number of relevant legal principles will also need to be borne in mind as crucial background context, regardless of the form of settlement pursued.

23.3.1 Legal professional privilege

Prosecuting authorities are increasingly requesting or encouraging corporates to waive privilege as a sign of their co-operation, or even as a precondition to concluding a settlement. The extent to which the prosecuting authority and a corporate may diverge in their interpretations or application of legal professional privilege (LPP) is dealt with in Chapter 35 but the appropriateness of putting pressure on a corporate to waive LPP is far from clear; particularly in the context of a multi-jurisdictional investigation where a number of different legal systems may be in play, all with varying degrees of protection for lawyer–client communications. The collateral damage to the corporate's interests in other jurisdictions if LPP were to be waived could potentially be substantial, and would need to be carefully considered before the corporate agreed to a global settlement involving a waiver on this basis. Attempts to resolve these difficulties by offering limited waiver may work but in practice are certainly not without risk (including, in particular, in relation to collateral waiver risks in jurisdictions that do not recognise limited waiver).

The SFO's guidance on corporate co-operation[91] states that a corporate that does not waive privilege and provide witness accounts will not attain the corresponding factor against prosecution found in the DPA Code, although the corporate will not be penalised by the SFO for electing against waiving privilege. This

89 *Three Rivers District Council and Others v. The Governor and Company of the Bank of England* [2003] EWCA Civ 474.

90 *Tchenguiz v. Director of the Serious Fraud Office (Non-Party Disclosure)*, also known as *Rawlinson and Hunter Trustees SA v. Akers* [2014] EWCA Civ 136 at para. 15.

91 Corporate Co-operation Guidance, issued by the SFO, on 6 August 2019.

guidance also states that, if a corporate claims privilege during an investigation, the SFO will expect it to 'provide certification by independent counsel that the material in question is privileged'. How this will work in practice remains to be seen.

Admissions 23.3.2

Unlike a plea agreement, the settlement of criminal proceedings by way of a CRO or DPA does not require the corporate to make formal admissions of guilt. However, the effect in practice of agreeing to a CRO or a DPA may be equivalent to an admission. An application for a CRO will be accompanied by a detailed statement of claim,[92] and by agreeing to the CRO the defendant may be taken as confirming its agreement to the contents. Similarly, whereas an admission is not a prerequisite for a DPA, once the DPA is approved, the statement of facts on which it is based becomes admissible in subsequent proceedings in England and Wales (not limited to related criminal proceedings) as if it were the corporate's admission of its contents.

Indirect admissions of this kind entail risk for both the corporate and any other persons concerned in the conduct. They could potentially be relied on by third parties in support of civil or criminal proceedings brought against the corporate, both in the United Kingdom and overseas. They are also likely to prejudice the position of any other persons concerned in the conduct, not limited to the corporate's officers. This exposure increases the more extensive the indirect admissions are. In negotiating the first UK DPA, the SFO considered it necessary for the statement of facts to be lengthy (in this instance, 55 pages) to put the judge in a position to approve the agreement on the most complete basis available. The other published approved statements of facts to date generally follow a similar approach.

A corporate could seek to avoid or at least mitigate some of these adverse consequences by concluding a settlement under which a subsidiary accepts liability and makes any necessary admissions, as in the MW Kellogg Limited CRO in 2011.[93] Note, however, that a corporate will not be able to hide behind a subsidiary that has been set up as a vehicle through which a corrupt payment may be made so that the subsidiary can be abandoned if the corrupt payment comes to light.[94] Alternatively, a corporate could seek to negotiate a settlement under which an individual officer accepts liability instead of the corporate. However, if there is a prospect of a successful prosecution of the corporate entity, this may be unlikely to succeed. As a general matter, risk mitigation strategies of this kind are likely to be highly context-specific, and subject to the willingness of the relevant prosecuting authorities to recognise the interests at stake.

92 Practice Direction – Civil Recovery Orders, at paras. 4.1 to 4.5.

93 'MW Kellogg Limited to pay £7 million in SFO High Court action', press release dated 16 February 2011, SFO.

94 *Serious Fraud Office v. XYZ Ltd* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509 at para. 28.

23.4 Practical issues arising from the negotiation of UK DPAs

DPAs have to date been made available only for a limited range of corporate economic offences prosecuted by either the CPS or the SFO. Statute governs eligibility for a DPA, its contents and the manner in which it is to be negotiated and approved, with limited discretion left to either the corporate or the prosecuting authority. This departure from the much more flexible US model complicates any predictions as to how frequently DPAs will be relied on in practice in the United Kingdom, but this section will consider practical issues arising from the negotiation of the first UK DPA as part of a global settlement.

The legislation requires the judge hearing the application to be satisfied that a DPA is in the interests of justice (as opposed to prosecution of the corporate). The first four DPAs agreed at the time of writing, *Standard Bank plc*, *XYZ Ltd (Sarclad)*, *Rolls-Royce* and *Tesco Stores Limited*, were all heard by Sir Brian Leveson, President of the Queen's Bench Division, who (as is clear from the judgments) went to considerable lengths to satisfy himself that the proposed DPAs were in the interests of justice and that the terms were fair, reasonable and proportionate. Notably in *Rolls-Royce* he said that the involvement of prosecutors in different countries (in this case, the United States and Brazil) should not preclude a DPA in the United Kingdom, but the extension of criminality to these countries is relevant to the balancing exercise of whether the DPA is in the interests of justice.[95] Following Leveson P's retirement in 2019, Davis J heard the fifth DPA, *Serco Geografix Limited*, and adopted a similar approach.

In the *Standard Bank* decision, Leveson P noted that the first consideration must be the seriousness of the conduct and in this regard emphasised that the potential criminality faced by the bank was the failure to prevent intended bribery committed by senior officers of a sister company. He also noted the SFO's conclusion that there was insufficient evidence to suggest that any of Standard Bank's employees had committed an offence. Nevertheless, in the *Rolls-Royce* DPA, Leveson P described the conduct of the company as some of the 'most serious' breaches of criminal law in the areas of bribery and corruption but found that a DPA was ultimately in the interests of justice because of the extent of other factors, demonstrating that, in certain circumstances, the seriousness of the conduct need not be a bar for a company looking to agree a DPA with the authorities. In particular, *Rolls-Royce* was unique because of the extent of the negative impact that a prosecution of the company would have had on employees and others innocent of any misconduct – factors that were taken into account by Leveson P when balancing the public interest and interests of justice in ultimately approving the DPA. The public interest factors in *Serco Geografix Limited* also outweighed the seriousness of the offence, despite Davis J describing it as 'a substantial fraud' reflecting business practices 'apparently ingrained in the company' and which was

95 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249 at para. 42.

compounded by the serious impact the conduct had on the integrity of the process of outsourcing public functions to private companies.[96]

Leveson P also attached considerable weight to the early report made by Standard Bank to the authorities, noted that the bank had made significant enhancements to its compliance policies and procedures since 2011 and that the bank in its form as at November 2015 was effectively a different entity from that which had been involved in the events that were the subject of the DPA. Notably, these two factors were also critical in the other four DPAs.[97] However, in *Rolls-Royce* there was no self-report; the SFO had been prompted to ask questions of the company by public postings on the internet. However, Rolls-Royce's co-operation with the SFO was praised by Leveson P, who found that the company could not have done more to expose its own misconduct, limited neither by time, jurisdiction nor area of business. It is this co-operation, in conjunction with extensive ethics and compliance measures and procedures that the company had put in place, and were committed to continuing, that was determinate in the agreement of a DPA, despite the lack of self-reporting.

In *Serco Geografix Limited,* Davis J also placed significant weight on the fact that Serco Geografix Limited was a dormant company, meaning that the obligations imposed on it under the DPA were of limited value, whereas the decision of its parent, Serco Plc, to provide undertakings 'of genuine and substantial effect' allowed the goals of the DPA to be achieved, which he described as an important development in the use of DPAs.[98]

DPA negotiations are held under strict confidentiality restrictions imposed by the SFO pursuant to the DPA Code of Practice. The Code of Practice requires the corporate entering into DPA negotiations to provide an undertaking in respect of the confidentiality of the fact the DPA negotiations are taking place.

What this means in practice is that third parties with whom the corporate needs to share the fact of the negotiations or any information relating to the DPA negotiations must sign a confidentiality undertaking. Any potential disclosure to the market has to be carefully considered and discussed with the SFO at an early stage (i.e., prior to the relevant obligation arising), and with the judge once an application to the court has been made.[99] Rule 5.8 Criminal Procedure Rules

96 *Serco Geografix Limited* [2019] 7 WLUK 45 at para. 22.

97 *Serious Fraud Office v. XYZ Ltd* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509 at paras. 15 to 18; *Rolls-Royce*, Crown Court (Southwark), 17 January 2017 at paras. 48 to 51, 60 and 63; *Tesco Stores Limited* (Case No. U20170287) [2017] 4 WLUK 558, at paras. 51 to 60; and *Serco Geografix Limited* [2019] 7 WLUK 45 at paras. 23, 25.

98 *Serco Geografix Limited* [2019] 7 WLUK 45 at para. 42: 'The nature of modern corporate structures means that it may be problematic to show that a controlling mind of the parent company was involved in the criminality carried out by a subsidiary company even where the benefit of the criminality tended to accrue to the parent company. Yet it will be the parent company which necessarily must engage in any compliance programme and cooperate with law enforcement agencies. The approach taken by Serco Group PLC in this case strengthens the public interest in the approval of this DPA.'

99 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249 at para. 14.

2015 stipulates that details of a court hearing must appear on the court list at most 48 hours before the court hearing, and the listing must include the names of the parties. This in itself may give rise to press and market speculation on the subject matter of the DPA and the size of the financial penalty. If an announcement is required, an application should be made to the nominated judge.

The legislation does not address anonymity of individuals in the statement of facts. There are protections afforded in US DPAs and in the course of FCA investigations by the third-party rights provisions, and by the 'Maxwellisation' process in public inquiries. In *Standard Bank plc*, the conclusion reached was that those named on the draft indictment would be named, as would be the bank's senior deal team member, but that the remaining individuals whose conduct was relevant to the factual narrative would remain anonymous. The potential consequences of the naming of individuals following the DPA's publication can be seen in the fact that Ms Shose Sinare, one of the Tanzanian individuals allegedly responsible for the underlying offence in *Standard Bank plc*, has brought a civil claim against Standard Bank in the Tanzanian courts alleging, among other things, that she had a right to see and respond to the allegations in the statement of facts.

Tesco Stores Limited and *XYZ Ltd (Sarclad)* are the only cases to date where the SFO has pursued charges against individuals following entry into a DPA. The DPA judgment in *Tesco Stores Limited* was embargoed for almost two years pending the conclusion of the prosecution of the three former employees, owing to the risk of the details of the DPA undermining or prejudicing those proceedings.[100] The first trial of the three former employees was abandoned after the former UK financial director suffered a heart attack. The former UK managing director and former UK food commercial director were retried and acquitted of all charges, after the trial judge ruled that they had no case to answer. The trial judge's decision was upheld, in emphatic terms, by the Court of Appeal. Subsequently, the former UK financial director, who had been severed from the retrial, was acquitted of all charges after the SFO offered no evidence, and the embargo on the DPA was lifted on the same day. Counsel for the three former employees had made representations to Leveson P, both before the DPA was approved and also before it was published, that the statement of facts should be published in a form that did not identify the three former employees, as it would be unfair for the individuals' names and the conduct ascribed to them in the DPA to be publicly available in perpetuity when they had not been found to have committed any offence. On each occasion the request was declined, on the basis that the statement of facts had been ratified by that stage and the legislation does not address anonymity of individuals.

XYZ Ltd (Sarclad) was anonymised on the basis that there were ongoing criminal proceedings arising out of the same facts; to avoid the risk of prejudice in those proceedings, the court ordered that the judgment providing full details of the parties involved only be made public following the conclusion of those

100 As Tesco plc had publicly announced entering into the DPA, and its quantum, pursuant to its regulatory obligations as a publicly listed company, no attempt was made to anonymise its identity.

proceedings.[101] Sarclad was a small company and was charged with both substantive offences, requiring the application of the identification principle through the involvement of very senior former employees, and for the offence of failing to prevent bribery under the Bribery Act, which may have related to both agents and employees. On 16 July 2019, all three defendants were acquitted of all counts and the judgment providing full details of the facts, the DPA and the statement of facts were published. As with the Tesco DPA, this has resulted in the individuals being identified in the publicly available DPA judgment (by role) and the statement of facts (by name) and said to have committed criminal offences, despite having been acquitted of all counts.

See Section 23.1

The *Tesco Stores Limited* and *XYZ Ltd (Sarclad)* DPAs have led to strong calls from a wide range of practitioners and commentators that consideration be given to introducing mechanisms to protect the interests of individuals in the DPA process. A DPA is likely to take less time than a contested trial, so the basis of the DPA will normally be determined before any trial of individuals, which creates a risk that the findings of fact will differ between the two. This risk arises whenever different people are the arbiters of fact, but it is heightened in these circumstances, as the DPA process requires close co-operation between the prosecutors and company to agree on the facts, whereas a trial is a judicially overseen adversarial process in which the jury decides any issues in dispute. Additionally, the company may not have access to the evidence of the natural persons under investigation at the time of a DPA negotiation (e.g., the enforcement agency may have requested the company not to interview the individuals or the individuals may have refused to answer questions at interview, for fear of self-incrimination) and may only come to understand their position if they enter the witness box.

Rolls-Royce did not include the identities of the individuals involved in the criminal conduct for the same reason of avoiding prejudice to potential criminal proceedings.[102] In addition to this, the Court did not name the recipients of corrupt payments or bribes in certain countries on the basis that that this could lead to action or the imposition of penalties which would be regarded in the UK as contravening Article 3 of the European Convention on Human Rights.[103] The *Rolls-Royce* DPA itself says in terms that it does not provide any protection against prosecution of any present or former officer, director, employee or agent of Rolls-Royce, and further, Rolls-Royce is required to co-operate with the investigation and prosecution of the individuals involved in the relevant conduct.[104] The SFO ultimately decided against prosecuting any individuals in the Rolls-Royce investigation.[105]

101 *Serious Fraud Office v. XYZ Ltd* (Case No. U20150856) [2016] 7 WLUK 220, [2016] Lloyd's Rep FC 509 at para. 3.

102 *Rolls-Royce* (Case No. U20170036) [2017] 1 WLUK 189, [2017] Lloyd's Rep FC 249 at para. 32.

103 Ibid. at para. 32.

104 Ibid. at paras. 71, 72.

105 https://www.sfo.gov.uk/2019/02/22/sfo-closes-glaxosmithkline-investigation-and-investigation-into-rolls-royce-individuals/.

The negotiation process in *Standard Bank plc* did not move as quickly as originally anticipated. It became apparent that an adversarial stance would not be appropriate in seeking to negotiate an agreement, and over time communications became more focused and more effective. It is also clear from the facts available that *XYZ Ltd (Sarclad)* and *Rolls-Royce* took considerable periods to resolve; so, while the process towards a DPA is likely to be shorter than a contested trial, it will probably still take a considerable period to agree and be approved.

Before the preliminary application is filed at court by the SFO, the corporate is required to provide a declaration regarding the information supplied to the SFO, as well as the declaration of the individual through whom the corporate made its declaration. The declarations are required to be made pursuant to the Criminal Procedure Rules 2015.[106]

To provide comfort to the corporate and the individual it may be necessary to follow a similar process to that used when individuals sign regulatory attestations – including understanding the documentation provided and questioning those involved in the data collection process. This is something to consider as early as possible in the DPA negotiations.

It is also clearly important to seek to ensure that the scope of any compliance review or monitorship is limited to the matters that are relevant to the circumstances of the case, as these can be intrusive, lengthy and costly exercises.

In global investigations and settlement discussions it is essential to keep in close contact with other investigating agencies, where necessary providing detailed explanations of the DPA process and the basis on which the statement of facts and DPA terms have been agreed.

23.5 Resolving parallel investigations

In the United Kingdom, historically civil proceedings were generally stayed pending the outcome of any parallel criminal proceedings. However, courts consider this approach case by case and the emphasis has increasingly moved away from the presumption of a stay. Specifically in the context of contemplated CROs, the current policy (set out in the Attorney General's Guidelines on asset recovery)[107] should prevent civil recovery proceedings from being pursued in parallel with criminal proceedings; although the Bruce Hall example discussed above demonstrates there is no bar against such proceedings being pursued in tandem with criminal proceedings provided the conduct that is the subject of the respective proceedings can be appropriately distinguished.[108]

106 Rule 11.2(3)(c) Criminal Procedure Rules 2015 No. 1490 (L.18).

107 Guidance for prosecutors and investigators on their asset recovery powers under Section 2A of the Proceeds of Crime Act 2002, 29 November 2012, Attorney General's Office.

108 cf. Thomas LJ in *Innospec*.

Other domestic authorities 23.5.1

We have already identified some of the difficulties of negotiating a truly 'global' settlement and their inherent limitations; many of which are equally relevant where there are multiple domestic authorities investigating the same conduct and both civil and criminal proceedings are in contemplation. Corporates seeking to reach a settlement with other domestic authorities are likely to be assisted by agreements and memoranda of understanding (MOU) already in place between the main authorities, including, for example, the MOU between the Competition and Markets Authority and the SFO,[109] and the FCA's Enforcement Guide.[110] The DPA agreed between the SFO and Tesco Stores Limited was coordinated with an agreement with the FCA that Tesco Stores Limited and its parent company, Tesco plc, had committed market abuse.[111] Leveson P did not order Tesco Stores Limited to pay any compensation as part of the DPA as the SFO had said that this would not be a straightforward position; the SFO had not been approached by any investor seeking compensation; and Tesco Plc and Tesco Stores Limited had previously agreed with the FCA to pay an estimated £84.4 million under a statutory compensation scheme. The UK criminal courts have historically been reluctant to determine complex issues of compensation and this case demonstrates how DPAs can work in conjunction with regulatory arrangements to compensate victims.

Foreign authorities 23.5.2

The interplay of agencies becomes even more complex where foreign agencies are involved. The participation of UK authorities in global settlements has to date typically been driven by the US authorities, reflecting the relative ease with which US prosecutors can establish corporate criminal liability. One potential issue arises from divergent and sometimes conflicting requests from authorities, typically in connection with communications, disclosure of materials and confidentiality. The aim of any settlement negotiations should be to encourage one authority to take the lead, in accordance with any applicable guidelines or agreements concluded by the relevant authorities for this purpose.

109 Memorandum of understanding between the Competition and Markets Authority and the Serious Fraud Office, 29 April 2014.

110 FCA Handbook, Enforcement Guide, E.G. 12 and E.G. Appendices 2 and 3.

111 'Tesco to pay redress for market abuse', press release, 28 March 2017, FCA.

24

Negotiating Global Settlements: The US Perspective

Nicolas Bourtin[1]

24.1 Introduction

Strong incentives exist for corporations – particularly those in highly regulated industries that are vulnerable to potentially debilitating collateral consequences – to avoid litigating a case brought by the government. Among other considerations, protracted and unpredictable litigation can create risks of (1) financial and reputational harm to the company, (2) weakening relationships with regulators, (3) significant legal expense, and (4) severe legal and regulatory consequences associated with an unfavourable litigation outcome. As a result, when threatened with enforcement action, corporations often seek to enter into settlement negotiations with investigating authorities. Nevertheless, a corporation entering into such negotiations must carefully weigh the various attendant burdens and collateral consequences of such agreements.

24.2 Strategic considerations

As a preliminary matter, it is important to consider the impact of all interactions with US authorities on the company's ability to reach a settlement on favourable terms. Even early in an investigation, a corporation can develop a co-operative working relationship with an enforcement agency through prompt and complete disclosure and assistance with requests and inquiries. While co-operation is not the right strategic approach in all cases – companies may choose to take a more adversarial approach, even early in an investigation – establishing a record of proactive and complete co-operation can have a substantial effect on the final terms

1 Nicolas Bourtin is a partner at Sullivan & Cromwell LLP. The author acknowledges the contributions of former Sullivan & Cromwell associates Kate Doniger, Stephanie Heglund and Ryan Galisewski to earlier editions of this chapter.

of any resolution, as US government authorities typically consider the nature and extent of a corporation's co-operation with the investigation in contemplating whether to settle a matter and on what terms. Indeed, both the US Department of Justice (DOJ) and the US Securities and Exchange Commission (SEC, or the Commission) have explicitly included voluntary disclosure and co-operation in their enforcement policies. As outlined in the DOJ's Justice Manual, in determining whether and to what extent to award a company co-operation credit, the DOJ considers, among other things, 'the timeliness of the co-operation, the diligence, thoroughness and speed of the internal investigation, and the proactive nature of the co-operation'.[2] Similarly, the SEC Enforcement Manual provides that a company's co-operation is evaluated by considering self-policing, self-reporting of misconduct, remediation and co-operation with the investigation.[3] As a result, by conducting an internal investigation and self-reporting potential misconduct to the authorities, a corporation may increase its chances of receiving co-operation credit and, in turn, more favourable settlement terms.[4]

At the close of the government's investigation, when beginning to negotiate the terms of a potential settlement agreement, a corporation must be particularly attuned to both the timing and the breadth of such an agreement. Regarding timing, certain stages of litigation can be particularly costly for a corporation; securing settlements early may be advantageous for a corporation. For example, in some cases – particularly where the key facts are known early and there is public pressure on the government to act quickly – a speedy settlement may be struck before a lengthy and expensive investigation is conducted. Such circumstances are rare, however, and the government will normally be reluctant to reach a settlement before a full investigation has been completed.

---

2 United States Department of Justice (DOJ) Justice Manual § 9-28.700, Principles of Federal Prosecution of Business Organizations, The Value of Cooperation (rev. November 2017); see also Justice Manual § 9-47.120, FCPA Corporate Enforcement Policy (added November 2017). On 20 November 2019, the DOJ announced further revisions to its Foreign Corrupt Practices Act Corporate Enforcement Policy that, while modest, reflect DOJ's commitment to providing incentives for companies to self-disclose suspected FCPA violation. The policy revision makes clear that a company's notice to the DOJ of potential criminal conduct can earn it self-reporting credit even if the company does not at the time of the notification understand the full scope of the conduct or the involvement of all relevant employees. In such circumstances, the DOJ will not later penalise the company's self-report for failure to include 'all relevant facts'.

3 SEC, Office of Chief Counsel, Enforcement Manual, Framework for Evaluating Cooperation by Companies § 6.1.2 (28 November 2017); see also SEC Release No. 44969, Report of Investigation Pursuant to Section 21(a), Exchange Act Release No. 44,969, 76 SEC Docket 220 of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions (23 October 2001); SEC Release No. 34-61340, Policy Statement Concerning Cooperation by Individuals, in its Investigations and Related Enforcement Actions Exchange Act Release No. 34-61340, 75 Fed. Reg. 3122-02 (13 January 2010), www.sec.gov/rules/policy/2010/34-61340.pdf (last accessed 12 November 2019).

4 See, e.g., Report of Investigation Pursuant to Section 21(a), Exchange Act Release No. 44,969, 76 SEC Docket 220 (23 October 2001) (declining to take action against the parent company given the company's response to the apparent misconduct and setting forth criteria the SEC considers in determining whether, and how much, to credit self-reporting).

Another pivotal point to consider is whether settlement can be achieved before indictment or the filing of a complaint, as such public actions carry the risk of significant legal, financial and reputational consequences. And in fact most negotiated corporate resolutions are reached before charges are filed, as companies are eager to avoid the uncertain public and shareholder reaction to a contested litigation. A recent economic study showed that a company's share price generally decreases more dramatically as a result of the announcement of a government investigation if there is no concurrent resolution.[5] The extent of share price declines can, among other effects, have great significance in follow-on civil litigation.

In terms of the breadth of a potential settlement agreement, a corporation must consider the scope of the conduct being investigated and the scope of the potential release from liability. At the conclusion of the government's investigation, to the extent that it opts to pursue charges related to certain alleged misconduct, it can be advantageous for those charges to be reflected in a single settlement agreement or in distinct agreements announced simultaneously, so as to mitigate the risk of legal, financial and reputational harm associated with multiple days of negative press, carry-over investigations and future litigation. In the event that the government determines not to pursue charges against the company or its employees,[6] it can be advantageous to diplomatically encourage a declination – a

5 See Declaration of Stephen Choi, Ph.D., *In re Goldman Sachs Grp., Inc. Sec. Litig.*, No. 1:10-cv-03461-PAC, 2015 WL 5613150 (S.D.N.Y. 6 April 2015), ECF No. 145 (finding that the average impact of an investigation announcement was -3.8 per cent when there was no concurrent resolution, compared to 0.22 per cent when there was a concurrent resolution). In one particularly striking example, Goldman Sachs settled a case for US$550 million in 2010 to avoid the difficulty and notoriety of litigation; after news of the settlement hit the market, Goldman's shares increased 5 per cent, resulting in a market value increase greater than the cost of the settlement. Sewell Chan & Louise Story, 'Goldman Pays $550 Million to Settle Fraud Case', *The New York Times* (15 July 2010), www.nytimes.com/2010/07/16/business/16goldman.html.

6 The Justice Manual lists 10 factors that prosecutors should weigh in determining whether to charge a corporation, including: (1) the nature and seriousness of the offence; (2) the pervasiveness of wrongdoing within the corporation; (3) the corporation's history of similar misconduct; (4) the corporation's willingness to co-operate including as to potential wrongdoing by its agents; (5) the existence and effectiveness of the corporation's pre-existing compliance programme; (6) the corporation's timely and voluntary disclosure of wrongdoing; (7) the corporation's remedial actions; (8) collateral consequences; (9) the adequacy of other remedies; and (10) the adequacy of the prosecution of individuals responsible for the corporation's malfeasance. Justice Manual § 9-28.300, Principles of Federal Prosecution of Business Organizations, Factors to Be Considered (rev. November 2018). The SEC considers its own factors in determining whether to close an investigation, including: (1) the seriousness of the conduct and potential violations; (2) the staff resources available to pursue the investigation; (3) the sufficiency and strength of the evidence; (4) the extent of potential investor harm if an action is not commenced; and (5) the age of the conduct underlying the potential violations. SEC, Office of Chief Counsel, Enforcement Manual § 2.6.1, Policies and Procedures.

formal notice that the government has declined to pursue the case further,[7] to provide the company valuable closure.

Owing to the government's focus on the prosecution of individuals, however, it is unlikely that the government will release from liability company employees who engaged in potential wrongdoing as part of a settlement with a company.[8] The DOJ formalised its increased focus on the prosecution of individuals with the publication of a 2015 policy memorandum signed by then-Deputy Attorney General Sally Quillian Yates regarding individual accountability for corporate wrongdoing.[9] The Yates Memorandum memorialised certain government sentiments demonstrating an inclination toward the prosecution of individuals in corporate fraud cases,[10] and specified that 'absent extraordinary circumstances or approved departmental policy, the Department will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation'.[11]

---

7 Precise practices may differ. The policy of the SEC, for example, is to send 'termination letters' to 'notify individuals and entities at the earliest opportunity when the staff has determined not to recommend an enforcement action against them to the Commission'. SEC, Office of Chief Counsel, Enforcement Manual § 2.6.2, Termination Notices. These SEC termination letters provide somewhat less assurance than a formal declination, because '[a]ll that such a communication means is that the staff has completed its investigation and that at that time no enforcement action has been recommended'. Id.

8 One exception is found in settlements with the DOJ's Antitrust Division. Historically, antitrust settlements regularly contained non-prosecution provisions that protected a company's employees from criminal liability related to the antitrust activity at issue. Antitrust settlements may 'carve out' certain individuals from this protection based on their level of culpability. See Sally Quillian Yates, Memorandum from the U.S. Dep't of Justice on Individual Accountability for Corporate Wrongdoing (9 September 2015), https://www.justice.gov/dag/file/769036/download.

9 Id.

10 See, e.g., Marshall Miller, Principal Deputy Assistant Attorney General for the Criminal Division, Remarks at the Global Investigations Review conference (17 September 2014), https://www.justice.gov/opa/speech/remarks-principal-deputy-assistant-attorney-general-criminal-division-marshall-l-miller (explaining that 'when [corporations] come in to discuss the results of an internal investigation to the Criminal Division . . . expect that a primary focus will be on what evidence you uncovered as to culpable individuals, what steps you took to see if individual culpability crept up the corporate ladder, how tireless your efforts were to find the people responsible'); Sung-Hee Suh, Deputy Assistant Attorney General, Remarks at the PLI's 14th Annual Institute on Securities Regulation in Europe: Implications for U.S. Law on EU Practice (20 January 2015), https://www.justice.gov/opa/pr/deputy-assistant-attorney-general-sung-hee-suh-speaks-pli-s-14th-annual-institute-securities (explaining that 'corporations do not act criminally, but for the actions of individuals . . . the Criminal Division intends to prosecute those individuals, whether they are sitting on a sales desk or in a corporate suite'); Leslie Caldwell, Assistant Attorney General for the Criminal Division, Remarks at New York University Law School's Program on Corporate Compliance and Enforcement (17 April 2015), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-new-york-university-law (explaining that '[t]rue cooperation . . . requires identifying the individuals actually responsible for the misconduct – be they executives or others – and the provision of all available facts relating to that misconduct').

11 Sally Quillian Yates, Memorandum from the U.S. Dep't of Justice on Individual Accountability for Corporate Wrongdoing at p. 2 (9 September 2015), https://www.justice.gov/dag/file/769036/download.

Following the change of administration in 2017, the DOJ revised the Yates Memorandum's guidance to restore some discretion to civil prosecutors, who are now empowered to 'negotiate civil releases for individuals who do not warrant additional investigation in corporate civil settlement agreements'.[12] The revised guidance also states that a corporation will be eligible for co-operation credit if it operates in good faith to identify individuals who were 'substantially' involved in or responsible for the potential misconduct, a move away from the Yates Memorandum's more stringent requirement that 'the company must identify all individuals responsible for the misconduct at issue, regardless of their position, status, or seniority'. However, the revised guidance emphasises the DOJ's ongoing commitment to and focus on individual accountability.[13]

Similarly, in the securities enforcement context, the SEC has expressed a focus on charging individuals responsible for wrongdoing.[14] In particular, Mary Jo White, the former Chair of the SEC, has highlighted that one new approach to charging individuals is to use Section 20(b) of the Exchange Act[15] to target those who have 'engaged in unlawful activity but attempted to insulate themselves from liability by avoiding direct communication with the defrauded investors'.[16]

24.3 Legal considerations

24.3.1 Privilege considerations

At times during the investigative process, legal considerations may be in tension with strategic ones – a corporation should be cognisant of the potential for such tensions to navigate toward an agreeable settlement without unnecessarily waiving

12 Rod J Rosenstein, Deputy Attorney General, Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0. When announcing these changes, Deputy Attorney General Rod Rosenstein emphasised that this policy shift was in 'response to concerns raised about the inefficiencies of requiring companies to identify every employee involved regardless of relative culpability' and was 'consistent with our commitment to hold individuals accountable in every appropriate case.' Id.

13 Id.

14 Joshua Gallu and David Michaels, SEC to Shift Enforcement Focus to Individuals, White Says, *Bloomberg News* (26 September 2013), www.bloomberg.com/news/articles/2013-09-26/sec-to-shift-enforcement-focus-to-individuals-white-says-1-; Mary Jo White, SEC Chair, Speech at the New York City Bar Association's Third Annual White Collar Crime Institute: Three Key Pressure Points in the Current Enforcement Environment (19 May 2014), https://www.sec.gov/news/speech/2014-spch051914mjw.html (noting that an 'internal, back-of-the[-]envelope, analysis the staff did recently indicates that since the beginning of the 2011 fiscal year, we charged individuals in 83% of our actions . . . , [a]nd we look for ways to innovate in order to further strengthen our ability to charge individuals').

15 Section 20(b) of the Securities Act of 1933 allows the Commission to bring enforcement actions against 'any person' who does 'any act or thing which it would be unlawful for such person to do under the provisions of this chapter or any rule or regulation thereunder through or by means of any other person'. See 15 U.S.C. § 78t(b) (2011).

16 Id.

any valuable rights. In particular, a company may need to weigh the value of additional co-operation credit for disclosing relevant privileged documents to the government against the value of protecting privileged documents from future discovery in follow-on civil litigation.

On the one hand, the government may consider the disclosure of privileged documents in determining the corporation's level of co-operation. Under current DOJ policy, for example, 'cooperation credit is not predicated upon the waiver of attorney–client privilege or work-product protection', although co-operation still requires the timely disclosure of 'relevant facts',[17] which may require the disclosure of some privileged materials, such as memoranda of witness interviews prepared during an internal investigation.[18] On the other hand, disclosure to the government of documents prepared during the course of an investigation may waive any relevant protections during follow-on civil litigation.[19] In such instances, a company may consider entering into a limited waiver agreement with the government as a middle ground, but it must keep in mind that courts may be sceptical of a limited waiver agreement, even when paired with a confidentiality agreement.[20]

17 Memorandum from Mark Filip, Deputy Att'y Gen., U.S. Dep't of Justice, Principles of Federal Prosecution of Business Organizations (28 August 2008), at pp. 9 to 11, https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf.

18 Id., at pp. 8, 9. This reflects a steady retreat in the DOJ's position. In 1999, then-Deputy Attorney General Eric Holder noted in a memorandum that the DOJ would consider the waiver of corporate attorney–client and work-product privileges as, although not an 'absolute requirement', at least 'one factor in evaluating the corporation's cooperation'. Memorandum from the DOJ on Bringing Criminal Charges Against Corporations §§ II.A.4, VI.A-B (16 June 1999), https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2010/04/11/charging-corps.PDF.
After some Congressional interest in corporate attorney–client privilege, the DOJ issued another memorandum in 2006 stating that, although '[w]aiver of attorney–client and work product protections is not a prerequisite to a finding that a company has cooperated', prosecutors could request carefully limited waivers only in limited circumstances 'when there is a legitimate need for the privileged information to fulfil their law enforcement obligations'. Memorandum from Paul J McNulty, Deputy Att'y Gen., U.S. Dep't of Justice, Principles of Federal Prosecution of Business Organizations (12 December 2006), at pp. 8, 9, https://www.justice.gov/sites/default/files/dag/legacy/2007/07/05/mcnulty_memo.pdf.

19 A court in the Southern District of New York recently held that briefs, written memos, white papers and presentations shown to the CFTC were discoverable in a subsequent civil action. See *Alaska Electrical Pension Fund v. Bank of America Corp.,* 2017 WL 280816, at *2, 3 (S.D.N.Y. 20 January 2017). The court's decision, however, noted the lack of confidentiality agreements between the government and the defendants, and the court did not claim to apply a categorical rule about confidentiality agreements and waiver of work-product privilege. See ibid., at *2. ('[T]he Court need not decide categorically whether confidentiality agreements can ever protect work product that is shared voluntarily with a government agency because, at most, they are just one of several factors to be considered, and they are not enough to carry the day here.') (Internal quotation marks and citations omitted.)

20 Most federal courts of appeal have declined to allow a selective disclosure to regulators during an investigation of documents protected by the attorney–client privilege or work-product doctrine without a resultant waiver of the privilege or protection with respect to third-party civil litigants. See *In re Pac. Pictures Corp*., 679 F.3d 1121 (9th Cir. 2012), at pp. 1127, 1128 (U.S. Attorney investigation); *In re Qwest Commc'ns Int'l, Inc.*, 450 F.3d 1179 (10th Cir. 2006)

Recent amendments to the SEC Enforcement Manual indicate that advocacy materials presented to the SEC may be discoverable and admissible in evidence, notwithstanding the protections of Federal Rules of Evidence 408 and 410.[21]

As part of its investigative process, the government may also engage the company in discussions as to whether charges are warranted. Government authorities may convey this information to the company orally, through reverse proffers,[22] or in writing, through a document such as the SEC's Wells notice.[23] Upon receipt of such information, the company then generally may respond with its arguments as to why the government should not bring an enforcement action. While providing a response is usually advisable and carries the prospect of success, in certain circumstances, a corporation may determine that it is not in the company's best interest. Among other considerations, a Wells submission is not privileged or confidential, and therefore can be used later against the corporation in civil litigation or made publicly available. In the alternative, the corporation may opt to initiate a meeting

(SEC and DOJ investigations); SEC, Office of Chief Counsel, Enforcement Manual § 4.3.1, Confidentiality Agreements (28 October 2016) ('While obtaining materials that are otherwise potentially subject to privilege or the protections of the attorney work-product doctrine can be of substantial assistance in conducting an investigation, the staff should exercise judgment when deciding whether to enter into a confidentiality agreement with a company under investigation. Considerations include [that] . . . [s]ome courts have held that companies that produce otherwise privileged materials to the SEC or the US Department of Justice, even pursuant to a confidentiality agreement, waived privilege in doing so.'). But see *In re Steinhardt Partners, L.P.,* 9 F.3d. 230 (2d Cir. 1993), at p. 236 ('[W]e decline to adopt a *per se* rule that all voluntary disclosures to the government waive work product protection . . . . Establishing a rigid rule would fail to anticipate . . . situations in which the SEC and the disclosing party have entered into an explicit agreement that the SEC will maintain the confidentiality of the disclosed materials.'); see also *In re Natural Gas Commodity Litigation*, 2005 WL 1457666, at *8 (S.D.N.Y. 21 June 2005) (discussing how an explicit confidentiality agreements combined with a non-waiver agreement went a 'long way' toward establishing non-waiver).

21 See SEC, Office of Chief Counsel, Enforcement Manual § 3.2.3.2, White Papers and Other Materials (excluding Wells submissions) (28 October 2016).

22 See Andrew Ceresney, Director, SEC Division of Enforcement, Remarks at University of Texas School of Law's Government Enforcement Institute: The SEC's Cooperation Program: Reflections on Five Years of Experience (13 March 2015), https://www.sec.gov/news/speech/sec-cooperation-program.html. ('One thing we are doing more of is using reverse proffers at key points in our investigations. When appropriate, we will invite counsel in for a meeting in which we share key documents and expected testimony that will implicate the defendant. This is another practice that is well established among criminal prosecutors and FBI agents but historically has been used less frequently at the SEC. Sometimes we might do a reverse proffer at a more advanced stage of an investigation in order to attempt to bring the investigation swiftly to a close on settlement terms that we deem favourable and appropriate. But we also might do it much earlier in an investigation, in order to demonstrate to a witness why cooperation is worthwhile.')

23 A Wells notice is a letter that a securities or commodities regulator, such as the SEC, the Commodity Futures Trading Commission (CFTC), or the Financial Industry Regulatory Authority (FINRA), sends to a corporation or individual when it intends to bring a civil action against them. See, e.g., *Richman v. Goldman Sachs Grp*., Inc., 868 F. Supp. 2d 261 (S.D.N.Y. 2012), at p. 272 ('The SEC provides a target of an investigation with a Wells Notice "whenever the Enforcement Division staff decides, even preliminarily, to recommend charges".') (Citation omitted.)

with the authorities to discuss the proposed charges, to prevent the creation of discoverable material and foster a dialogue between the company and the government.

During settlement negotiations, a corporation must also be careful in sharing drafts of settlement documents because materials shared with the government may become discoverable in civil litigation. Although Federal Rule of Evidence 408 generally protects documents related to settlement negotiations,[24] the documents may nonetheless ultimately be deemed discoverable,[25] or even admissible as evidence.[26]

Limitations and tolling agreements 24.3.2

In the course of a government investigation, statutes of limitation will often come into play.[27] At the outset of an investigation, particularly if the investigation commences toward the end of a particular statutory period, the government may ask the company to sign a tolling agreement, an agreement to waive a right to claim that litigation should be dismissed owing to the expiry of a statute of limitations for a particular period. It may be in the best interest of the company to sign it, as a form of co-operation and to avoid a precipitous filing of charges by the government. If a tolling agreement has not been signed at an earlier stage in the investigation, the government may ask a corporation to sign one during the settlement negotiation process, especially if a potential limitations period is about to close. In this context, tolling agreements serve to relieve the government of the pressure of taking formal action before the relevant limitations period runs, and allow for time for additional sharing of information in the hope of facilitating a settlement agreement.[28]

---

24 See Fed. R. Evid. 408 advisory committee's note. ('[S]tatements made during compromise negotiations of other disputed claims are not admissible in subsequent criminal litigation, when offered to prove liability for, invalidity of, or amount of those claims.')

25 For example, courts in the Southern District of New York consistently hold that 'Rule 408 does not apply to discovery'. E.g., *Small v. Nobel Biocare USA, LLC*, 808 F. Supp. 2d 584 (S.D.N.Y. 2011), at p. 586; accord *Conopco, Inc. v. Wein*, 2007 WL 1040676, at *5 (S.D.N.Y. 4 April 2007); *ABF Capital Mgmt. v. Askin Capital*, 2000 WL 191698, at *1 (S.D.N.Y. 10 February 2000). Rather, courts apply the discovery standard of Federal Rule of Civil Procedure 26(b)(1) to determine the discoverability of settlement negotiations. E.g., *Small*, 808 F. Supp. 2d at pp. 586, 587; *ABF Capital Mgmt.*, 2000 WL 191698, at *2. Some courts require a 'particularized showing' of the need for the discovery. See *Bottaro v. Hatton Assocs.*, 96 F.R.D. 158 (E.D.N.Y. 1982), at p. 160; see also *Tribune Co. v. Purcigliotti*, 1996 WL 337277, at *2 (S.D.N.Y. 19 June 1996) ('slightly heightened showing of relevance'); *SEC v.* Thrasher, 1996 WL 94533, at *2 (S.D.N.Y. 27 February 1996) ('modest presumption against disclosure').

26 E.g., *In re Gen. Motors LLC Ignition Switch Litig.*, 2015 WL 7769524, at *2 (S.D.N.Y. 30 November 2015) (admitting consent decree as evidence 'not . . . to prove that New GM violated the Safety Act . . . but for other purposes that are plainly relevant').

27 Unless otherwise provided by statute, an enforcement action by a federal regulator that seeks a civil fine or penalty is generally subject to the standard five-year limitations period for proceedings. 28 U.S.C. § 2462.

28 See SEC, Office of Chief Counsel, Enforcement Manual § 3.1.2, Statutes of Limitations and Tolling Agreements (28 October 2016). ('If the assigned staff investigating potential violations of the federal securities laws believes that any of the relevant conduct arguably may be outside the five-year limitation period before the SEC would be able to file or institute an enforcement

24.4 Forms of resolution

24.4.1 Prosecutorial settlements: DPAs, NPAs and guilty pleas

In past years, most corporate criminal investigations initiated by US prosecutors were resolved by deferred prosecution agreements (DPAs) and non-prosecution agreements (NPAs).[29] DPAs and NPAs are generally thought of as a middle ground between declining prosecution and obtaining a conviction.[30] Although in

---

action, the staff may ask the potential defendant or respondent to sign a "tolling agreement." Such requests are occasionally made in the course of settlement negotiations to allow time for sharing of information in furtherance of reaching a settlement.').

A tolling agreement signed by the corporation will not toll the statute of limitations against individuals. Rather, to toll the time to bring charges against an individual, the government will have to secure a separate tolling agreement with that person. See Sally Quillian Yates, Memorandum from the U.S. Dep't of Justice on Individual Accountability for Corporate Wrongdoing at p. 6 (9 September 2015) ('[W]here it is anticipated that a tolling agreement is . . . unavoidable and necessary, all efforts should be made either to resolve the matter against culpable individuals before the limitations period expires or to preserve the ability to charge individuals by tolling the limitations period by agreement or court order.'), https://www.justice.gov/dag/file/769036/download.

29 For examples of DPAs and NPAs, see *In re Legg Mason, Inc*. (4 June 2018), https://www.justice.gov/criminal-fraud/file/1072461/download (NPA, FCPA claims); *In re Credit Suisse* (24 May 2018), https://www.justice.gov/criminal-fraud/file/1079596/download (NPA, FCPA claims); *In re Las Vegas Sands Corp*. (17 January 2017), https://www.justice.gov/opa/press-release/file/929836/download (NPA, FCPA claims); *In re Gen. Cable Corp*. (DOJ, 22 December 2016), https://www.justice.gov/criminal-fraud/file/921801/download (NPA, FCPA claims); *In re JPMorgan Securities (Asia Pacific)* (DOJ, 17 November 2016), https://www.justice.gov/criminal-fraud/file/911356/download (NPA, FCPA claims); *In re IAP Worldwide Servs. Inc.* (DOJ, 16 June 2015), https://www.justice.gov/opa/file/478281/download (NPA, FCPA claims); *In re Dallas Airmotive, Inc.* (DOJ, 10 December 2014), https://www.justice.gov/file/181831/download (DPA, FCPA claims); *In re HSBC Holdings plc* (10 December 2012), https://www.justice.gov/sites/default/files/opa/legacy/2012/12/11/dpa-executed.pdf (DPA, IEEPA & TWEA claims); *In re ING Bank N.V.* (8 June 2012), https://www.sec.gov/Archives/edgar/data/1039765/000119312513120728/d501093dex45.htm (DPA, IEEPA & TWEA claims); *In re Wells Fargo Bank, N.A.* (DOJ, 8 December 2011), https://www.justice.gov/sites/default/files/atr/legacy/2011/12/08/278076a.pdf (NPA, anticompetitive conduct claims); *In re Tenaris S.A.* (DOJ, 17 May 2011), https://www.sec.gov/news/press/2011/2011-112-dpa.pdf (DPA, FCPA claims); *In re Barclays Bank PLC* (DOJ, 16 August 2010), www.federalreserve.gov/newsevents/press/enforcement/enf20100818b1.pdf (DPA, IEEPA & TWEA claims); *In re ABN AMRO Bank N.V.* (DOJ, 9 May 2010), (DPA, IEEPA & TWEA claims); *In re Wachovia Bank, N.A.* (DOJ, 16 March 2010), https://www.sec.gov/litigation/complaints/2011/comp22183.pdf (DPA, money laundering claims).

30 See Justice Manual § 9-28.1100, Principles of Federal Prosecution of Business Organizations, Collateral Consequences (rev. November 2015) ('[W]here the collateral consequences of a corporate conviction for innocent third parties would be significant, it may be appropriate to consider a non-prosecution or deferred prosecution agreement with conditions designated, among other things, to promote compliance with applicable law and prevent recidivism. Such agreements are a third option, besides a criminal indictment, on the one hand, and a declination, on the other.'); see also Mary Jo White, SEC Chair, Speech at the New York City Bar Association's Third Annual White Collar Crime Institute: Three Key Pressure Points in the Current Enforcement Environment (19 May 2014), https://www.sec.gov/news/speech/2014-spch051914mjw.html. ('[S]ome have questioned whether it is appropriate for prosecutors to consider the consequences – direct and collateral – when they make a decision whether to indict a company. Of course

recent years there have been some high-profile corporate guilty pleas, there is no indication yet that these guilty pleas will overtake NPAs and DPAs as prosecutors' primary settlement mechanism.[31]

In a deferred prosecution, the government brings criminal charges against the company, which it agrees to dismiss at the end of a specified period if the company complies with the DPA's terms. Because a DPA is filed with the court, it becomes a public document.

A non-prosecution differs in that no criminal charges are filed against the company. As a result, an NPA need not be made public unless prosecutors seek to publicise the results of the investigation or the company is itself required to disclose the agreement. The DOJ commonly uses both forms of agreement to resolve investigations concerning, among other things, fraud, the Foreign Corrupt Practices Act,[32] the False Claims Act,[33] the Bank Secrecy Act[34] and antitrust laws. In previous years, DPAs and NPAs were the exclusive domain of the DOJ, but the SEC and state prosecutors have also recently adopted their use, using the agreements to resolve certain securities law violations.[35]

Unlike an NPA, over which the government has full discretion to adopt terms and conditions, a DPA may be subject to some level of judicial review pursuant to the Speedy Trial Act. Because a DPA involves the filing of an information or indictment, the Speedy Trial Act requires trial to start within 70 days.[36] However, the Speedy Trial Act allows this 70-day period to be tolled with the 'approval of the court, for the purpose of allowing the defendant to demonstrate his good

---

they should; we want their decision to be thoughtful and in the public interest. And the DOJ's Principles of Federal Prosecutions of Business Organizations indeed require them to weigh the collateral consequences of a corporate indictment among a number of other factors.')

31 Although there is no standard form or precedent for these agreements, most prosecutorial settlement agreements include some or all of the following provisions: (1) a statement of facts describing illegal acts and/or an admission of wrongdoing; (2) an agreement that the company, its employees and its agents will not publicly contradict the statement of facts; (3) co-operation with the government for the duration of the agreement, including the provision of documents and efforts to secure employee testimony; (4) some form of remedial action, including terminating or disciplining culpable employees, implementing revised internal controls and procedures, and/or, in some cases, appointing an independent compliance monitor; (5) fines and penalties; (6) obligations to report future violations of law; and (7) an acknowledgement that the government has the sole discretion to determine whether the agreement has been breached. For both an NPA and a DPA, because the company has generally admitted to the conduct at issue, if a company is indicted upon breach of the agreement, conviction is almost certain.

32 15 U.S.C. §§ 78dd-1, et seq.

33 31 U.S.C. §§ 3729-3733.

34 31 U.S.C. §§ 5311–5330.

35 Andrew Ceresney, Director, SEC Division of Enforcement, Remarks at University of Texas School of Law's Government Enforcement Institute: The SEC's Cooperation Program: Reflections on Five Years of Experience (13 March 2015), https://www.sec.gov/news/speech/sec-cooperation-program.html; Enforcement Cooperation Program, SEC (16 February 2016), https://www.sec.gov/spotlight/enfcoopinitiative.shtml.

36 See 18 U.S.C. § 3161(c)(1); see also Justice Manual: Criminal Resource Manual § 628, Speedy Trial Act of 1974 (rev. November 2015).

conduct'.[37] Although this provision suggests that courts have a role in overseeing DPAs, judges have historically been relatively deferential to the government in approving them.

Two recent decisions from the Courts of Appeals for the DC and Second Circuits confirm that the long-standing practice of limited judicial oversight over consensual enforcement settlements is the favoured approach. In each case, the district court refused to approve a settlement that the court deemed too lenient, and was reversed by the Court of Appeals on the grounds that the trial court's discretion in such circumstances is quite limited. In April 2016, in *United States v. Fokker Services BV*,[38] the DC Circuit Court of Appeals issued a writ of *mandamus* and vacated a decision by District Judge Richard Leon, rejecting as too lenient a proposed DPA between the DOJ and Fokker Services. The Court of Appeals reasoned that 'the court's withholding of approval would amount to a substantial and unwarranted intrusion on the Executive Branch's fundamental prerogatives'.[39] Similarly, in June 2014, the Second Circuit issued a decision in *SEC v. Citigroup Global Markets*,[40] calling into question the appropriateness of judicial scrutiny of consensual settlements with the SEC. In a decision that reversed a notable opinion written by Judge Jed Rakoff criticising an SEC settlement with Citigroup as insufficient, the Second Circuit made clear that courts must afford the SEC's policy judgements 'significant deference', including whether, when and how to resolve enforcement proceedings. Under *Citigroup*, a district court's review of a settlement agreement is narrow and limited.[41] Subsequent cases have added glosses to the *Citigroup* holding, with some district courts exerting discretion over certain aspects of settlement agreements,[42] including the selection of an independent monitor.[43]

Despite the reversals, the district courts' criticisms are broadly consistent with those expressed in recent years by a number of federal judges who have hesitated before ultimately approving DPAs and other similar government settlements. In those other instances, the courts' criticisms commonly have included assertions

37 18 U.S.C. § 3161(h)(2).

38 818 F.3d 733 (D.C. Cir. 2016), at p. 747, vacating 79 F. Supp. 3d 160 (D.D.C. 2015).

39 Id., at p. 744.

40 752 F.3d 285 (2d Cir. 2014). The Second Circuit further emphasised this holding in a recent decision, *United States v. HSBC Bank*, which overturned a district court's decision to unseal a monitor's report and found that the district court erred in involving its supervisory authority over the DPA. 863 F, 3d 125 (2d Cir. 2017).

41 Id., at p. 294 (quoting *eBay, Inc. v. MercExchange*, 547 U.S. 388 (2006), at p. 391).

42 See, e.g., *U.S. Securities and Exchange Commission v. Aronson*, 665 F. App'x 78 (2d Cir. 2016), at p. 80 (holding that the district court did not abuse its discretion in ordering briefing on an issue before a related criminal case was completed, even though the consent decree provided that the parties would propose a briefing schedule after the completion of the criminal case).

43 See *U.S. Commodity Futures Trading Commission v. Deutsche Bank* AG, 2016 WL 6135664, at *1 to 3 (S.D.N.Y. 20 October 2016) (holding that it was proper for the court to select an independent monitor, when the parties' proposed monitors were inadequate).

that those settlements lacked (1) a large enough penalty amount[44] (relatedly, there is concern that companies will begin to view monetary penalties merely as 'a cost of doing business'[45]), (2) admissions of wrongdoing by the company,[46] (3) charges against the individuals who were responsible for the offence,[47] (4) sufficient factual detail for the judge to evaluate the agreement,[48] (5) sufficient remedial obligations for the company[49] and (6) sufficient reporting to the court about the company's compliance with the agreement.[50]

In recent years, perhaps as a result of political and public pressure,[51] including such public criticism of DPAs from the federal courts, there has been an uptick in guilty pleas to resolve criminal actions.[52] The major difference between a guilty plea and an NPA or DPA is that a guilty plea results in a conviction, which

44 See *U.S. v. Saena Tech Corp*., 140 F. Supp. 3d 11 (D.D.C. 2015), at p. 31. ('An agreement that contained neither punitive measures (such as fines) nor requirements designed to deter future criminality (such as compliance programs and independent monitors) could not be said to be designed to secure a defendant's reformation and should be rejected. Even an agreement that contained some of these elements could be ineffective if the obligations were found to be so vague or minimal as to render them a sham.')

45 See, e.g., Brett Wolf, 'U.S. Warns Banks It May Revoke Some Money-Laundering Settlements', Reuters (15 March 2015), http://www.reuters.com/article/us-banks-moneylaundering-idUSKBN0MC1ZE20150316 (quoting Assistant Attorney General Caldwell as saying 'We don't want DPAs and NPAs to be perceived as a cost of doing business'); Peter J Henning, 'Guilty Pleas and Heavy Fines Seem to Be Cost of Business for Wall St.', *The New York Times* (20 May 2015), https://www.nytimes.com/2015/05/21/business/dealbook/guilty-pleas-and-heavy-fines-seem-to-be-cost-of-business-for-wall-st.html?_r=0. ('Banks appear willing to plead guilty as long as the collateral costs are not too heavy. Thus, the potency of a criminal conviction as a deterrent seems to have been dissipated, perhaps to the point that it is just another business expense.')

46 See, e.g. *S.E.C. v. CR Intrinsic Investors, LLC*, 939 F. Supp. 2d 431 (S.D.N.Y. 2013), at pp. 436 to 439 (discussing concerns about allowing 'neither admit nor deny' provisions in a consent judgment).

47 See *Saena Tech Corp*., 140 F. Supp 3d at 35-36 (discussing potential concerns with a DPA that effectively immunised an individual).

48 Cf. *U.S. Securities and Exchange Commission v. Mulvaney*, 2012 WL 12930425, at *1 (E.D. Wis. 20 November 2012) (granting consent decree only after ordering further briefing on its factual basis).

49 See *Saena Tech Corp*., 140 F. Supp. 3d at p. 31 (discussing the necessity of sufficient deterrent effects).

50 Cf. *U.S. v. HSBC Bank USA, N.A.*, 2013 WL 3306161, at *11 (E.D.N.Y. 1 July 2013) (ordering the parties to file quarterly reports and stating that it will 'notify the parties if, in its view, hearings or other appearances are necessary or appropriate').

51 See, e.g., Danielle Douglas, 'Holder Concerned Megabanks Too Big to Jail', *The Washington Post* (6 March 2013), https://www.washingtonpost.com/business/economy/holder-concerned-megabanks-too-big-to-jail/2013/03/06/6fa2b07a-869e-11e2-999e-5f8e0410cb9d_story.html.

52 Notably, in May 2015 Citicorp, JPMorgan Chase & Co., Barclays PLC, Royal Bank of Scotland and UBS all pleaded guilty in May 2015 to felony charges for conspiring to manipulate foreign exchange benchmark rates. 'Five Major Banks Agree to Parent-Level Guilty Pleas', press release, DOJ (20 May 2015), https://www.justice.gov/opa/pr/five-major-banks-agree- parent-level-guilty-pleas; see also DB Group Servs. Plea Agreement, 3:15CR62 (D. Conn. 23 April 2015), https://www.justice.gov/file/628871/download; BNP Paribas S.A. Order to Cease and Desist (Fed. Reserve Sys. 30 June 2014),

generally comes with harsher collateral regulatory consequences and more significant reputational harm. Such risks for a corporation are significant, especially in a heavily regulated industry – the ramifications can be wide-ranging and unclear.

See Section 24.5.3

24.4.2 Regulatory settlements: consent orders and civil NPAs and DPAs

Companies under investigation by federal and state regulators whose enforcement mechanisms are administrative or civil may resolve an investigation by voluntarily entering into a consent order where an institution typically consents to the issuance of a cease-and-desist order or the assessment of a civil monetary penalty, or both. A consent order, like a cease-and-desist order or a civil monetary penalty assessment, is a formal enforcement action; it is a public document and, although it may not always be filed, its terms are enforceable in court. Consent orders often vary in the level of detail they provide concerning the wrongdoing, although they are often less detailed than a criminal settlement. A consent cease-and-desist order may oblige the company to undertake remedial measures to correct the misconduct and ensure future compliance. The term of the order is usually indefinite. A consent civil monetary penalty assessment merely obliges the institution to pay a penalty, and the order's terms are fully satisfied by the payment.

Some regulators have adopted NPAs and DPAs that are similar to their criminal counterparts'. For example, the SEC, which is responsible for civil enforcement and administrative actions to enforce the securities laws,[53] has begun to use NPAs and DPAs to resolve cases 'where an entity or person has engaged in misconduct and where the co-operation is extraordinary, but the circumstances call for a measure of accountability'.[54] Although available as an option, NPAs and DPAs remain relatively uncommon for civil enforcement actions by the SEC.[55]

24.5 Key settlement terms

Whether negotiating a settlement agreement in the criminal or regulatory context, many common principles come into play. To facilitate a successful negotiation, a company must have a comprehensive understanding of (1) benchmark terms for

https://www.federalreserve.gov/newsevents/press/enforcement/enf20140630a1.pdf; Credit Suisse AG Plea Agreement, 1:14-cr-00188 (E.D. Va. 19 May 2014), https://www.justice.gov/iso/opa/resources/6862014519191516948022.pdf; Marubeni Corporation (March 2014).

53 See SEC, How Investigations Work (rev. 15 July 2013), https://www.sec.gov/News/Article/Detail/Article/1356125787012; Mary Jo White, SEC Chair, Speech, 'All-Encompassing Enforcement: The Robust Use of Civil and Criminal Markets to Police the Markets' (31 March 2014), https://www.sec.gov/News/Speech/Detail/Speech/1370541342996.

54 Andrew Ceresney, Director, SEC Division of Enforcement, Remarks at University of Texas School of Law's Government Enforcement Institute, The SEC's Cooperation Program: Reflections on Five Years of Experience (13 March 2015), https://www.sec.gov/news/speech/sec-cooperation-program.html.

55 Id. ('[T]hey have been a relatively limited part of our practice. I think this is appropriate and should continue to be the case.'); see also SEC, Office of Chief Counsel, Enforcement Manual § 6.2.3, Non-Prosecution Agreements (28 October 2016). ('A non-prosecution agreement is a written agreement . . . entered in limited and appropriate circumstances.')

historical settlements regarding similar misconduct, (2) those terms that are most significant to the company and (3) any distinguishing factors in the matter at issue that encourage terms less severe than the benchmarks.

Monetary penalties 24.5.1

Nearly all corporate settlements with US authorities include some form of monetary penalty. The form largely depends on the regulator and its practices.[56] Typically, monetary penalties in regulatory settlements consist of a civil monetary penalty. Disgorgement of profits or restitution to harmed parties may also be required.[57]

The SEC considers two principal factors in determining monetary penalties: the presence or absence of a direct and material benefit to the corporation itself as a result of the violation and the degree to which the penalty will recompense or further harm the injured shareholders.[58] The SEC will also consider factors such as deterring the conduct, the extent of the injury, any complicity on the part of the corporation, the intent of the individuals committing the wrong, the difficulty in detecting that particular type of wrongdoing, any remedial steps taken by the corporation and the extent of its co-operation.[59] Generally, the factors that US authorities consider in determining monetary penalties mirror those used to determine whether to bring charges against the corporation in the first place, including the nature of the offence, the company's timely and voluntary disclosure of wrongdoing, and the company's remedial actions.

While settlement values generally increased between 2010 and 2015, there is some indication that this trend may be slowing, at least with respect to DOJ actions. For example, from 2005 to 2015, the total criminal fines and penalties assessed by the DOJ's Antitrust Division increased an entire order of magnitude,

56 See, e.g., Cornerstone Research, SEC Enforcement Activity Against Public Company Defendants: Fiscal Years 2010–2015, www.law.nyu.edu/sites/default/files/SEC-Enforcement-Activity-FY2010-FY2015.pdf. The SEC's monetary fines generally fall into three categories: (1) monetary penalties, (2) disgorgement with prejudgment interest, and (3) monetary relief for harmed investors. Id.

57 Forfeiture, the seizure of assets that comprised the proceeds of the wrongdoing, or were used to facilitate it, is rarely used in regulatory actions against business entities even when available, because the government is generally reluctant to seize property related to an ongoing business. See Justice Manual § 9-111.124 (Business Seizures ('Due to the complexities of seizing an ongoing business and the potential for substantial losses from such a seizure, a United States Attorney's Office must consult with the Asset Forfeiture and Money Laundering Section prior to initiating a forfeiture action against, or seeking the seizure of, or moving to restrain an ongoing business.')). Restitution, the compensation of individuals harmed by illegal conduct, is also rarely a part of any settlement. In particularly complex cases involving many different classes of individuals that may have been harmed, calculation of restitution may be especially difficult, and a corporation may find the government amenable to not seeking restitution in its settlement, with the understanding that compensation of harmed individuals is more efficiently and accurately handled through related civil litigation.

58 SEC Release No. 2006-4 (4 January 2016), Statement of the Securities and Exchange Commission Concerning Financial Penalties, https://www.sec.gov/news/press/2006-4.htm.

59 Id.

from US$338 million in 2005 to US$3.6 billion in 2015.[60] However, the total decreased to US$399 million in fiscal year 2016[61] and to US$67 million in 2017, and in 2018, the total was US$172 million.[62] In 2018, the DOJ collected more than US$2.8 billion in settlements and judgments from civil cases involving fraud and false claims against the government – the lowest recovery total since 2009.

The SEC has also increased its use of 'aggressive' monetary penalties in a trend that appears to be continuing.[63] Whereas a record-setting penalty in 2002 reached a mere US$10 million, the mean payment for certain cases between 2010 and 2013 was over US$50 million.[64] Three of the top 10 monetary settlements imposed in public company-related actions were imposed in 2016.[65] These include a US$415 million action against Merrill Lynch and a US$267 million action against JP Morgan wealth management subsidiaries. As of October 2016, SEC enforcement settlements related to misconduct leading to or arising from the financial crisis exceeded US$3.76 billion for the 204 entities and individuals charged.[66] An important June 2017 decision that may diminish the SEC's leverage in settlement negotiations is *Kokesh v. SEC*,[67] in which the Supreme Court held that a five-year statute of limitations applies to SEC enforcement actions seeking disgorgement.[68] The decision also raises the question of whether the Court would, in fact, recognise disgorgement as an available remedy in SEC enforcement

60 DOJ, Total Criminal Fines and Penalties (updated 28 January 2019), https://www.justice.gov/atr/total-criminal-fines.

61 Id.

62 Id.

63 SEC Enforcement Activity Against Public Companies and Their Subsidiaries, Cornerstone Research (2016), https://www.cornerstone.com/GetAttachment/1a6f93a7-3859-4e7e-841f-65241c49c123/SEC-Enforcement-Activity-against-Public-Companies.pdf.

64 Sonia A Steinway, Comment, SEC 'Monetary Penalties Speak Very Loudly,' But What Do They Say? A Critical Analysis of the SEC's New Enforcement Approach, 124 Yale L.J. 209 (October 2014) (analysing SEC trends in monetary penalties).

65 SEC Enforcement Activity Against Public Companies and Their Subsidiaries: Fiscal Year 2016 Update, Cornerstone Research (2016), https://www.cornerstone.com/Publications/Reports/SEC-Enforcement-Activity-Against-Public-Company-Defendants-2016.

66 SEC, SEC Enforcement Actions: Addressing Misconduct That Led To or Arose From the Financial Crisis, key statistics (22 February 2017), www.sec.gov/spotlight/enf-actions-fc.shtml (summarising all settlements resulting from the financial crisis). Other regulatory agencies have followed suit, with the CFTC enforcing a record US$3.144 billion in civil monetary penalties and US$59 million in restitution and disgorgement in 2015. Between 2010 and 2014, the New York Department of Financial Services (NYDFS) issued monetary penalties totalling near US$6 billion. Completed mainly through consent orders, NYDFS's most notable settlements include a US$600 million penalty against Deutsche Bank and a US$2.243 billion penalty against BNP Paribas, which eventually pleaded guilty to criminal charges and paid a total of US$8.9 billion to resolve the numerous investigations.

67 137 S. Ct. 1635 (2017).

68 Id., at 1645. Prior to this ruling, the SEC relied disproportionately on disgorgement penalties: in 2015, the SEC obtained US$3 billion in disgorgement payments and US$1.2 billion in other civil monetary penalties. See SEC, 'Select SEC & Market Data: Fiscal 2015' (2016), https://www.sec.gov/reportspubs/select-sec-and-market-data/secstats2015.pdf.

proceedings.[69] In 2017, the SEC collected US$1.2 billion in settlements with public companies and subsidiaries, almost all of it within the first half of the year, and in 2018, the SEC collected US$2.4 billion in settlements, more than the total in any fiscal year since 2010.[70]

The DOJ recently announced a written policy formalising how the Criminal Division should consider a company's argument that it is financially unable to pay an otherwise appropriate penalty.[71] Under the new policy, which aims to promote transparency around corporate penalties, the parties must first agree on the form of a corporate criminal resolution and the otherwise appropriate monetary penalty in the absence of the inability-to-pay considerations. The company must then complete an 11-point questionnaire, which requires the disclosure of, among other things, cash-flow projections, federal income tax returns for the past five years, operating budgets, acquisition or divestiture plans, encumbered assets and payments to the business's highest-earning executives.[72] DOJ lawyers are then directed to consider that information in light of statutory sentencing factors, the US Sentencing Guidelines, and the Justice Manual's principles regarding the consideration of collateral consequences in resolving a corporate criminal case.[73]

See Chapter 26 on fines, disgorgement, etc.

Continuing obligations 24.5.2

In addition to monetary penalties, settlement agreements will often include other continuing obligations. In particular, settlement agreements almost always contain language stating that the company will commit to undertake remedial efforts, such as the enhancement of its compliance programmes or an obligation to report potential violations of law in the future. To ensure ongoing compliance and

69 Id., at 1642, n. 3 ('Nothing in this opinion should be interpreted as an opinion on whether courts possess authority to order disgorgement in SEC enforcement proceedings or on whether courts have properly applied disgorgement principles in this context. The sole question presented in this case is whether disgorgement, as applied in SEC enforcement actions, is subject to § 2462's limitations period.'). See also Transcript of Oral Argument at 7 to 9, *Kokesh*, 137 S. Ct. 1635 (No. 16-529). Not surprisingly, the Supreme Court recently agreed to take up that very question. On 1 November 2019, the Supreme Court granted certiorari in *Liu v. SEC*, No. 18-1501, to decide whether the SEC may obtain disgorgement as 'equitable relief' in a civil action to enforce securities law violations. Should the Supreme Court conclude that the SEC has no such authority, absent a legislative fix, the SEC will be further limited in its ability to collect large financial awards in enforcement actions filed in court. The SEC would maintain such authority, however, in administrative actions, where the SEC's right to seek disgorgement is expressly authorised by statute.

70 SEC Enforcement Activity Against Public Companies and Their Subsidiaries, Cornerstone Research (2017), https://www.cornerstone.com/Publications/Reports/SEC-Enforcement-Activity-2017-Update; SEC Enforcement Activity Against Public Companies and Their Subsidiaries, Cornerstone Research (2018) (https://www.cornerstone.com/Publications/Reports/SEC-Enforcement-Activity-2018-Update).

71 Memorandum from Brian A Benczkowski, Assistant Att'y Gen., U.S. Dep't of Justice, Evaluating a Business Organization's Inability to Pay a Criminal Fine or Criminal Monetary Penalty (8 October 2019), https://www.justice.gov/opa/speech/file/1207576/download.

72 Id. at Attachment A.

73 Id. at p. 1.

satisfactory remedial efforts, in recent years, government agencies have increasingly required the use of corporate monitors to keep corporations accountable.

See Chapter 32 on monitorships

One common obligation in corporate settlements is the imposition of a monitor to oversee a company's compliance with a settlement agreement and report back to the government on the company's progress. Monitorships, which may last for a number of years, are a financial and functional burden on a company. Monitorships can be draining in terms of the cost of retaining the monitor itself, the costs required to implement recommended reforms, the cost of staffing and maintaining an internal team to work closely with the monitor and the disruption to the company's business and management. Another important consideration when contemplating a monitorship as a term of settlement is that monitors are generally given broad access to the corporation's files, outside the protection of an attorney–client relationship. This lack of attorney–client relationship can pose a risk of further legal exposure for the company. Given that a monitor is tasked with reviewing the corporation's practices, and reporting the findings of the review to relevant authorities, it is possible that the monitor will identify and be obliged to disclose additional violations of law to relevant authorities. In addition, once a monitor's reports are submitted to the relevant authorities, those reports and any documents contained in them can be subject to Freedom of Information Act requests, which may create additional exposure in follow-on civil litigation.

Given the substantial expense and disruption caused by a monitorship, it is in a corporation's interest to try and avoid the imposition of a monitor – especially in instances where corporate culpability is relatively low and the company has already undertaken substantial remedial efforts. The most effective means for a company of avoiding the imposition of a monitor continue to be to voluntarily report its misconduct, to co-operate fully with the government's resulting investigation and to demonstrate to the government that the company has already undertaken a comprehensive remediation plan. Where a monitor is imposed, a corporation can mitigate the disruption by negotiating the monitor's duration of assignment, scope of responsibility, decision-making capacity and accessibility to corporate files.

24.5.3 Collateral consequences

A criminal or regulatory settlement can also trigger a number of collateral consequences, which can vary depending on the types of violations the settlement covers and the industry of the affected entity. For example, a guilty plea for a bank could mean the loss of its financial holding company status and federal deposit insurance, the appointment of a receiver or conservator, and, for foreign banks, the potential termination of offices in the United States. A guilty plea for a broker-dealer could mean automatic loss of broker-dealer registration, a bar from acting as a registered investment adviser, and revocation of its status as a well-known seasoned issuer. A guilty plea for a corporation could also result in, among other things, disqualification from membership of certain self-regulatory organisations, a temporary or permanent bar from participation in federal procurement contracts (debarment), or loss of state licences. Compounding these

difficulties, many of the collateral consequences that arise upon conviction travel within a corporation's legal structure, so that even regulated businesses that were not involved in the offence can be subject to licence revocations, loss of securities law safe harbours and other consequences.

Corporations may need to seek waivers or exemptions from multiple regulators, including the SEC, the Commodity Futures Trading Commission, the Federal Reserve, the Department of Labor and the Financial Industry Regulatory Authority, to allow them to continue engaging in the affected business activities, a process that should be planned well in advance of settlement. Each regulator may have more than one relevant exemption.[74] The company will therefore need to assess the relevant regulations for each authority that oversees the company's activities. The permutations of collateral consequences are many and depend on the form of the settlement (e.g., DPA, NPA, guilty plea, conviction or consent order)[75] or even the nature of the offence.[76] In addition to automatic disqualifications, there is a wide array of discretionary actions available to regulators for which waivers or exemptions could be sought.[77]

The method of receiving a waiver or exemption from these collateral consequences depends on the agency. For the SEC, a corporation requests an exemption from the SEC Staff, which can either make a recommendation to the Commission or act directly on the application with delegated authority from the Commission.

74 The SEC has many, including: (1) status as a well-known seasoned issuer (WKSI); (2) status under § 9(a) of the 1940 Act as an investment adviser, depositor or principal underwriter of registered investment companies; and (3) exemptions from certain capital-raising restrictions, under Regulations A and D. See also generally Richard A Rosen and David S Huntington, 'Waivers from the Automatic Disqualification Provisions of the Federal Securities Laws', *29 Insights: The Corp. & Sec. Law Advisor* at p. 2 (August 2015) (cataloguing various SEC waivers).

75 Naturally, criminal convictions have much more severe consequences than a DPA, NPA or administrative consent order. For instance, Section 9(a) of the Investment Company Act of 1940 automatically bars an entity from acting as investment adviser or providing certain other services to registered investment companies if that entity or an affiliated entity has been convicted within the past ten years of any felony or misdemeanour arising out of the conduct of the business of a bank. 15 U.S.C. § 80a-9(a)(1).

76 For example, under the Commodities Exchange Act, an entity may be disqualified from registration under the Act if the entity has been found to have committed some kind of fraud by a settlement agreement with any federal or state agency. 7 U.S.C. § 12a(2), (3); see also No Action and Interpretation, Letter No. 12-70 (CFTC 31 December 2012), www.cftc.gov/idc/groups/public/@lrlettergeneral/documents/letter/12-70.pdf. The SEC has a policy of not enforcing the disqualifications under Section 206(4) of the Investment Advisers Act for administrative (but not civil) orders. See No-Action Letter, Dougherty & Co., 2003 WL 22204509 (SEC 3 July 2003).

77 For example, under Section 15(b)(4) of the Securities Exchange Act, the SEC has the discretion after a conviction to suspend or revoke the registration of a broker-dealer if it finds, after notice and comment, that it is in the public interest. See 15 U.S.C. § 78o(b)(4)(B).

The SEC generally grants a waiver under a finding of 'good cause'.[78] In contrast, the Department of Labor, in granting exemptions for qualified professional asset manager status, engages in a formal rule-making process, including a public notice and comment period.[79] The Federal Reserve, which can take a range of discretionary actions, generally engages in a more informal regulatory-relations dialogue when considering the collateral consequences of a significant settlement.

Timing is critical for the waiver process, because a company will need to ensure that there is no gap in its licences and statuses. Complicating matters, regulators often take different views as to when statutory disqualifications based on convictions or settlements commence. The SEC views 'conviction' as entry into a guilty plea, so any relevant SEC waivers need to be lined up before then. In contrast, the Department of Labor says that conviction is at sentencing, which can take place well after the entry of the guilty plea. For this reason, sentencing after the entry of a guilty plea can be delayed for the purpose of obtaining the necessary exemption from the Department of Labor.[80]

In recent years, the granting of waivers in connection with corporate settlements has drawn criticism by some in the government and the media that enforcement agencies have been too lenient in releasing companies from the consequences of their settlements, particularly in the case of companies that have been the subject of multiple enforcement actions.[81] There is every reason to believe that going forward the relevant agencies will require increasingly high showings by companies before agreeing to grant the necessary waivers.

78 17 C.F.R. § 230.405, Ineligible Issuer § 2 ('An issuer shall not be an ineligible issuer if the Commission determines, upon a showing of good cause, that it is not necessary under the circumstances that the issuer be considered an ineligible issuer.'); see also SEC, Div. of Corp. Fin., Revised Statement on Well-Known Seasoned Issuer Waivers (24 April 2014), www.sec.gov/divisions/corpfin/guidance/wksi-waivers-interp-031214.htm.

79 29 C.F.R. pt. 2570, subpt. B.

80 For example, in the set of plea agreements associated with manipulating foreign exchange benchmark rates, there was a term that the United States would support any motion or request to delay sentencing until the Department of Labor had issued a ruling on the request for exemption. E.g., Barclays Plea Agreement, Case No. 3:15CR00077 (D. Conn. 20 May 2015), at para. 12(e), https://www.justice.gov/file/440481/download; UBS Plea Agreement, Case No. 3:15CR00076 (D. Conn. 20 May 2015), at para. 28, https://www.justice.gov/file/440521/download.

81 See, e.g., Letter from Office of Sen. Elizabeth Warren, Rigged Justice: 2016: How Weak Enforcement Lets Corporate Offenders Off Easy (January 2016), https://www.warren.senate.gov/files/documents/Rigged_Justice_2016.pdf (describing major criminal and civil cases from 2015 in which report authors found government enforcement 'feeble' and insufficient to deter corporate crime); Kara M Stein, SEC Commissioner, Dissenting Statement in the Matter of the Royal Bank of Scotland Group, plc, Regarding Order Under Rule 405 of the Securities Act of 1933, Granting a Waiver from Being an Ineligible Issuer (28 April 2014), www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541670244 ('I fear that the Commission's action to waive our own automatic disqualification provisions arising from RBS's criminal misconduct may have enshrined a new policy – that some firms are just too big to bar.').

Admissions and follow-on civil litigation 24.5.4

With increasing frequency, as a condition of settlement, government authorities are requiring corporations to make factual or legal admissions, or both. For example, prior to 2013, the SEC had a long-standing policy of settling cases without requiring admissions from defendants.[82] In June 2013, however, following public criticism, including in the wake of Judge Rakoff's denial of approval of the SEC's settlement with Citigroup, the Commission changed its policy 'by requiring admissions of misconduct in certain cases where heightened accountability and acceptance of responsibility by a defendant are appropriate and in the public interest'.[83] The SEC has defined these types of cases as including instances (1) where the violation of the securities laws involved particularly egregious conduct, (2) where large numbers of investors were harmed, (3) where the markets or investors were placed at significant risk, (4) where the conduct obstructs the Commission's investigation, (5) where an admission can send an important message to the markets or (6) where the wrongdoer poses a particular future threat to investors or the markets.[84] Nevertheless, the SEC has also acknowledged that 'for reasons of efficiency and other benefits', including getting significant relief, eliminating litigation risk, returning money to victims expeditiously and conserving enforcement resources for other matters, 'most cases will continue to be resolved on a "neither admit not deny" basis'.[85] Indeed, even under the new policy, admissions still appear to be infrequent.[86]

In addition to the reputational impact and collateral consequences that such admissions can impose on a corporation, admissions can expose a company to significant liability in follow-on civil litigation. Plaintiffs may be able to rely on factual or legal admissions in settlement agreements to support a complaint,[87]

82 See SEC Release No. 33-337, Consent Decree in Judicial of Administrative Proceedings, 1972 WL 125351 (28 November 1972) (formally permitting respondent to avoid admitting or denying the allegations).

83 Andrew Ceresney, Director, SEC Division of Enforcement, Testimony on Oversight of the SEC's Division of Enforcement (19 March 2015), https://www.sec.gov/news/testimony/031915-test.html.

84 Id.; see also Mary Jo White, SEC Chair, Speech for the Council of Institutional Investors fall conference in Chicago, IL, 'Deploying the Full Enforcement Arsenal' (26 September 2013), https://www.sec.gov/News/Speech/Detail/Speech/1370539841202.

85 Id.

86 As at October 2015, according to one count, the SEC had only required admissions of fact in 18 settlements. See Marc S Raspanti et al., 'The SEC's New Admissions Policy Means Sometimes Having to Say You're Sorry', *The Champion* 16 (September/October 2015), at p. 17.

87 The following decisions allowed plaintiffs to rely on admissions made in a prior government settlement agreement: *Davis v. Beazer Homes, U.S.A. Inc.*, 2009 WL 3855935, at *7 (M.D.N.C. 17 November 2009) (finding company's statement in DPA was a significant factor contributing to the validity of plaintiff's claim); *Somerville v. Stryker Orthopedics*, 2009 WL 2901591, at *3 (N.D. Cal. 4 September 2009) (determining defendant's prior NPA contributed to the sufficiency of plaintiff's claim).

and may attempt to introduce them as evidence later.[88] A corporation will have a strong argument that an administrative consent order does not represent an adjudication and cannot be relied on in a complaint;[89] DPAs and NPAs have been used in follow-on litigation with mixed results.

A corporation entering into a settlement agreement ideally should, to the extent possible, try and neither admit nor deny the charges, in which case the findings of the order are less likely to be able to be used against it.[90] In the event that a corporation is unable to do so, a company should strategically negotiate for narrowly tailored factual statements and flexible language to enable it to defend itself in follow-on civil litigation. In particular, admitting to a generalised violation of law may be less likely to have future adverse consequences than admission of a specific legal violation that shares elements of claims that could be brought in follow-on civil litigation. For example, a corporation could admit to various controls-based violations in a settlement with the SEC rather than admitting to securities fraud. Or, a corporation could admit to a violation that does not contain a *scienter* element or does not concede that anyone was harmed as a result – necessary elements for many private causes of action.

Furthermore, a corporation should be aware that settlement agreements that dictate that the corporation cannot contradict the findings of facts can restrict the corporation's positions in follow-on civil litigation.[91] Because any statement that

88 E.g., *In re Gen. Motors LLC Ignition Switch Litig.*, 2015 WL 7769524, at *2 (S.D.N.Y. 30 November 2015) (admitting consent decree as evidence 'not . . . to prove that New GM violated the Safety Act . . . but for other purposes that are plainly relevant').

89 For example, the Second Circuit has held that 'a consent judgment between a federal agency and a private corporation which is not the result of an actual adjudication of any of the issues . . . can not be used as evidence in subsequent litigation between that corporation and another party'. *Lipsky v. Commonwealth United Corp.*, 551 F.2d 887 (2d Cir. 1976), at p. 893; see also *Waterford Tp. Police & Fire Ret. Sys. v. Smithtown Bancorp, Inc.*, 2014 WL 3569338 (E.D.N.Y. 18 July 2014) (striking from complaint references to consent agreements with the Federal Deposit Insurance Corporation and the New York Banking Department); *In re Platinum & Palladium Commodities Litig.*, 828 F. Supp. 2d 588 (S.D.N.Y. 13 September 2011) (striking from complaint references to CFTC's findings of fact contained in an administrative consent order). But see *In re Bear Stearns Mortg. Pass-Through Certificates Litig.*, 851 F. Supp. 2d 746 (S.D.N.Y. 2012), at p. 768 n. 24 ('[S]ome courts in this district have stretched the holding in *Lipsky* to mean that any portion of a pleading that relies on unadjudicated allegations in another complaint is immaterial under Rule 12(f). Neither Circuit precedent nor logic supports such an absolute rule.') (citation omitted); *Tobia v. United Grp. of Cos., Inc.*, 2016 WL 5417824, at *3 (N.D.N.Y. 22 September 2016) (holding that while the SEC complaint and consent order are inadmissible to prove liability under *Lipsky*, the allegations and findings enumerated in the SEC complaint are not made inadmissible merely by virtue of their inclusion therein).

90 See, e.g., *J.P. Morgan Securities Inc. v. Vigilant Ins. Co.*, 126 A.D.3d 76 (N.Y. App. Div. 1st Dep't 2015) (holding the insurer could not rely on the 'Dishonest Acts Exclusion' of policies to avoid indemnification of US$160 million disgorgement and US$90 million civil penalties required by an SEC cease-and-desist order).

91 See, e.g., *In re IAP Worldwide Services Inc.*, NPA, FCPA claims (DOJ, June 2015), https://www.justice.gov/opa/file/478281/download ("The Company admits, accepts, and acknowledges that it is responsible under United States law for the acts of its officers, directors, employees, and agents as set forth in the Statement of Facts . . . and that the facts described

could be viewed by the government as contradictory to the facts of the agreement may then be seen as a breach – thereby reviving a prosecutorial or regulatory action – it is important that such agreements, at a minimum, contain exceptions that allow a company to take good-faith positions in follow-on civil litigation.[92]

Resolving parallel investigations 24.6

Other domestic authorities 24.6.1

Most large-scale investigations of corporations involve a number of government agencies from federal and state governments, both prosecutorial and regulatory. The degree of coordination among these agencies varies case by case, and coordinating with multiple agencies can be challenging. However, there can be benefits to coordinated settlements, including closure for the company, enhanced legal certainty and the avoidance of unnecessary duplication,[93] or undue burdens of disclosure.[94] In addition, because the settlement announcements can occur on a single day, a company may be better able to control the release of information concerning the settlements and thereby limit the effect of any harmful disclosures on the market.[95] There is a distinct trend toward more and more multi-agency

. . . are true and accurate.'); c.f. SEC Release No. 9453, Order Instituting Cease-and-Desist Proceedings, *In the Matter of TD Bank, N.A.* (23 September 2013), https://www.sec.gov/litigation/admin/2013/33-9453.pdf (clarifying that '[t]he findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding').

92 See, e.g., *In the Matter of Citibank, N.A.*, CFTC Docket No. 16-16 (25 May 2016), at p. 26, www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcitibankisdaorder052516.pdf. ('Respondent agrees that neither it nor any of its successors and assigns, agents, or employees under its authority of control shall take any action or make any public statement denying directly or indirectly, any findings or conclusions in this Order or creating, or tending to create, the impression that this Order is without a factual basis; provided, however, that nothing in this provision shall affect Respondent's (i) testimonial obligations, or (ii) right to take positions in other proceedings to which the Commission is not a party.')

93 On 12 June 2018, the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation released a 'Policy Statement on Interagency Notification of Formal Enforcement Actions.' The statement requires the agencies to notify each other of enforcement actions against financial institutions, especially when the action they are pursuing involves the interests of another agency. If two or more of the agencies consider bringing complementary actions, they 'should coordinate the preparation, processing, presentation, potential penalties, service, and follow-up' of the enforcement action. A legislative effort to require eight federal agencies, including the DOJ and the SEC, to implement policies and procedures to minimise duplication of enforcement actions against financial institutions was approved by the US House of Representatives but was never voted on in the Senate.

94 SEC, press release, 'CFTC Sign Agreement to Enhance Coordination, Facilitate Review of New Derivative Products' (11 March 2008), https://www.sec.gov/news/press/2008/2008-40.htm.

95 See, e.g., SEC, press release, 'JPMorgan Chase Agrees to Pay $200 Million and Admits Wrongdoing to Settle SEC Charges' (19 September 2013), https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539819965 ('As part of a coordinated global settlement, three other agencies also announced settlements with JPMorgan today: the UK Financial Conduct Authority, the Federal Reserve, and the Office of the Comptroller of the Currency.'); SEC, press release, 'Standard Bank to Pay $4.2 Million to Settle SEC Charges' (20 November 2015),

settlements, as agencies increase collaboration, even across borders.[96] Recently, the DOJ announced a new policy intended to encourage coordination between it and other enforcement agencies and to discourage the disproportionate enforcement of laws by multiple authorities. Among other things, the new policy sets forth factors that DOJ attorneys may evaluate in determining whether multiple penalties serve the interests of justice in a particular case, including the egregiousness of the wrongdoing and the adequacy and timeliness of a company's disclosures and co-operation.[97] It remains to be seen to what degree this policy will result in meaningful changes to the DOJ's approach to settling investigations involving multiple agencies.

---

https://www.sec.gov/news/pressrelease/2015-268.html; SEC, press release, 'VimpelCom to Pay $795 Million in Global Settlement for FCPA Violations' (18 February 2016), https://www.sec.gov/news/pressrelease/2016-34.html. ('"This closely coordinated settlement is a product of the extraordinary efforts of the SEC, Department of Justice, and law enforcement partners around the globe to jointly pursue those who break the law to win business," said Kara N. Brockmeyer, Chief of the SEC Enforcement Division's FCPA Unit.')

96 Recent examples of multi-agency settlements include *In Re: Volkswagen 'Clean Diesel' Marketing, Sales Practices, and Products Liability Litigation*, 3:15-mc-02672-CRB (N.D. Cal. 17 May 2017) (consent decree with the DOJ, on behalf of the EPA and stipulated order for permanent injunction and monetary judgment for the FTC); *SEC v. Teva Pharmaceutical Industries, Ltd.*, 1:16-cv-25298 (S.D. Fla. 22 December 2016), https://www.sec.gov/litigation/litreleases/2016/lr23708.htm (DPA with the DOJ and interest and disgorgement payments to the SEC in connection with civil and criminal violations of the Foreign Corrupt Practices Act); SEC Release No. 78989, Order Instituting Administrative and Cease-and-Desist Proceedings (29 September 2016) (Och-Ziff DPA with the DOJ and interest and disgorgement payments to the SEC to resolve criminal charges arising out of bribes paid to public officials in the Democratic Republic of Congo and Libya), https://www.sec.gov/litigation/admin/2016/34-78989.pdf; Commerzbank AG Plea Agreement (D.D.C. 12 March 2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/12/commerzbank_deferred_prosecution_agreement_1.pdf (DPAs with the DOJ and DANY and consent orders with OCC and FinCEN); JPMorgan Chase Bank, N.A. Deferred Prosecution Agreement (S.D.N.Y. 6 January 2014), https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/JPMC%20DPA%20Packet%20%28Fully%20Executed%20w%20Exhibits%29.pdf (DPA with the DOJ and consent orders with the Federal Reserve, OFAC and NYDFS); SEC Release No. 9453, Order Instituting Cease-and-Desist Proceedings, In the Matter of TD Bank, N.A. (23 September 2013), https://www.sec.gov/litigation/admin/2013/33-9453.pdf (consent orders with the OCC and FinCEN and cease-and-desist order with SEC).

97 DOJ, Deputy Attorney General Rod Rosenstein Delivers Remarks to the New York City Bar White Collar Crime Committee (Remarks as prepared for delivery) (9 May 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

Foreign authorities 24.6.2

Owing at least in part to the internationalisation of enforcement, the global nature of modern-day securities frauds, increased regulatory activity on the state level and the increased complexity of the markets,[98] regulatory investigations today tend to involve a variety of authorities.[99] Thus a corporation must carefully evaluate whether a settlement with certain authorities should be postponed until a global resolution can be reached. Coordinated global settlements often afford the company the opportunity to predict and prevent excessive, cumulative or unnecessary monetary penalties, continuing obligations and collateral consequences.[100]

98 Mary Jo White, SEC Chair, Speech at the New York Bar Association's Third Annual White Collar Crime Institute, 'Three Key Pressure Points in the Current Enforcement Environment' (19 May 2014), https://www.sec.gov/news/speech/2014-spch051914mjw.html.

99 Examples of global settlements involving regulators from multiple jurisdictions include Odebrecht SA and Braskem SA Plea Agreements, see DOJ, press release, 'Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History' (21 December 2016), https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve (plea agreements with the DOJ, in which Odebrecht and Braskem agreed to pay a combined total penalty of at least $3.5 billion to resolve charges with authorities in the US, Brazil and Switzerland arising out of their schemes to pay hundreds of millions of dollars in bribes to government officials around the world); *SEC v. Embraer S.A.*, see SEC, press release, 'Embraer Paying $205 Million to Settle FCPA Charges' (24 October 2016), https://www.sec.gov/news/pressrelease/2016-224.html (DPA with the DOJ, and interest and disgorgement payments to the SEC and Brazilian authorities to resolve criminal and civil charges arising out of bribery of government officials in the Dominican Republic, Saudi Arabia and Mozambique, and the false recording payments in India via a sham agency agreement); *SEC v. VimpelCom Ltd*, see SEC, press release, 'VimpelCom to Pay $795 Million in Global Settlement for FCPA Violations' (18 February 2016), https://www.sec.gov/news/pressrelease/2016-34.html (settlement with US and Dutch regulators, with significant assistance from Norwegian, Swedish, Swiss, and Latvian authorities); Citicorp, JPMorgan Chase & Co., Barclays PLC and The Royal Bank of Scotland plc Plea Agreements, see DOJ, press release, 'Five Major Banks Agree to Parent-Level Guilty Pleas' (20 May 2015), https://www.justice.gov/opa/pr/five-major-banks-agree-parent-level-guilty-pleas (global settlement of claims against five banks involving DOJ, the Federal Reserve, CFTC and the New York State Department of Financial Services in the US, and the Financial Conduct Authority in the UK).

100 For example, as part of a global settlement regarding Odebrecht, the DOJ's plea agreement provided that 'the United States will credit the amount that Odebrecht pays to Brazil and Switzerland over the full term of their respective agreements.' DOJ, press release, 'Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History' (21 December 2016), available at https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve. And, as part of a global settlement with Embraer to resolve alleged FCPA violations, the SEC announced that 'Embraer may receive up to a $20 million credit depending on the amount of disgorgement it will pay to Brazilian authorities in a parallel civil proceeding in Brazil.' SEC, press release, 'Embraer Paying $205 Million to Settle FCPA Charges' (24 October 2016), https://www.sec.gov/news/pressrelease/2016-224.html.

25

Fines, Disgorgement, Injunctions, Debarment: The UK Perspective

Kelly Hagedorn, Robert Dalling and Matthew Worby[1]

25.1 Criminal financial penalties

Criminal offences of fraud, bribery and money laundering are covered by sentencing guidelines (the Guidelines) whether the offender is a company or an individual, and whether the conviction follows an investigation by the Serious Fraud Office (SFO), the National Crime Agency (NCA), Her Majesty's Revenue and Customs (HMRC), or other law enforcement authority.[2] The Guidelines apply in England and Wales and must be followed unless the court is satisfied that to do so would be contrary to the interests of justice.[3]

The Guidelines apply to all sentences passed on or after 1 October 2014, regardless of the date of the offence, and regardless of the date of the legislation under which the prosecution is brought (such as the Fraud Act 2006, the Proceeds of Crime Act 2002, and the Bribery Act 2010 (and their predecessors)).[4] In applying the Guidelines to offences prosecuted under legislation that pre-dates them, the court may reflect 'modern attitudes' to historic offences and make due

1 Kelly Hagedorn is a partner, Robert Dalling is special counsel and Matthew Worby is an associate at Jenner & Block London LLP. The authors wish to acknowledge the contributions of Peter Burrell, Simon Osborn-King and Paul Feldberg, the original authors of the chapter in previous editions, on which this chapter is partly based.

2 The Sentencing Council's Definitive Guideline for Fraud, Bribery and Money Laundering, published on 31 January 2014, available at https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-Bribery-and-Money-Laundering-offences-definitive-guideline-Web.pdf. We further note that the Sentencing Council is introducing a general sentencing guideline, effective from 1 October 2019, to cover offences that are not already the subject of a pre-existing guideline (available at https://www.sentencingcouncil.org.uk/overarching-guides/magistrates-court/item/general-guideline-overarching-principles/).

3 s.125, Coroners and Justice Act 2009.

4 See p. 4, the Guidelines.

allowance for any change in maximum sentence for that particular offence, to ensure that the sentence passed is in the interests of justice.[5] While in some cases that can result in an increase in penalty, in others it may mean a decrease. For example, under the Bribery Act the maximum sentence is 10 years' imprisonment, whereas before it had been seven.[6] On that basis, it could be argued that a fine for a pre-Bribery Act offence calculated using the new Guidelines should be discounted by up to 42 per cent to reflect that while the Guidelines apply to pre- and post-Bribery Act conduct, the fine should recognise that Parliament intended conduct after the Bribery Act came into force to be punished more severely.

The Guidelines set out a step-by-step guide to be used by the court in assessing the sentence to be imposed on individuals and corporates. Set out below are the steps the sentencing court must follow when assessing the penalties to impose on a corporate defendant for offences of fraud, money laundering and bribery.

Compensation 25.2

The court must first consider whether any compensation should be paid by the company to the victim for any personal injury, loss or damage resulting from the offence.[7] The amount of the order will be the amount the court considers appropriate, having regard to any evidence and to any representations made by or on behalf of the offender (or prosecutor).[8] In respect of such claims, the SFO will need to provide evidence to the court of a request for compensation by the victim. In the case of *R v. Smith & Ouzman Ltd*,[9] Recorder Mitchell QC indicated that he would have refused the SFO's request for a compensation order, as the SFO had not produced evidence of a request for compensation from the victim.

The making of a compensation order is not mandatory, but the court should provide reasons as to why it has not made one.[10] The court must have regard to the financial means of the defendant. If the defendant's means are limited, priority should be given to the payment of compensation over any other financial penalties.

Confiscation 25.3

Confiscation must be considered if either the Crown asks for it or the court thinks that it may be appropriate.[11] The aim of confiscation is to deprive defendants of the benefit that they have gained from their criminal conduct,[12] and it is irrelevant for the purposes of calculating a benefit figure whether the defendant has retained the benefit of his or her conduct. The benefit figure will represent the total value of the benefit obtained by the defendant, although the final confiscation order

5 *R v. Hall* [2011] EWCA Crim 2753; *R v. Clifford* [2014] EWCA Crim 2245.
6 s.11, Bribery Act 2010.
7 s.130(1)(a), Powers of Criminal Courts (Sentencing) Act 2000.
8 s.130(4), Powers of Criminal Courts (Sentencing) Act 2000.
9 Unreported, Southwark Crown Court, 7 January 2015.
10 s.130(3), Powers of Criminal Courts (Sentencing) Act 2000.
11 The Guidelines, p. 48.
12 s.6, Proceeds of Crime Act 2002.

cannot be for a greater sum than the value (at the time the order is made) of (1) the assets the defendant has available and (2) any property transferred by the defendant during the six years preceding the date of charge, for less than market value (tainted gifts). The court must address the following factors before making a confiscation order: (1) whether the defendant has benefited from the criminal conduct; (2) the value of the benefit obtained; and (3) the sum that is recoverable from the defendant.[13]

The application of the confiscation regime as regards the calculation of benefit has become less harsh in recent years. In corruption cases, for example, a prosecutor could previously have claimed that the benefit obtained was the entire value of the contract won through the criminal conduct, and request that that amount be confiscated. However, recent case law indicates that a 'judge should, if confronted by an application for an order which would be disproportionate, refuse to make it but accede only to an application for such sum as would be proportionate'[14] when calculating the amount of an offender's benefit. When the offender is a company, this should be restricted to gross profit earned together with any other pecuniary advantage flowing from the corruption.[15] In a separate case, it has been held that where the defendant can establish that VAT output tax on revenue obtained from criminal conduct has been properly accounted for to HMRC, it would be disproportionate to make a confiscation order calculated on the basis that a sum equivalent to that VAT paid has been 'obtained' by the defendant.[16]

When calculating the gross profit, the approach is typically to 'add back' the amount of bribes paid that may have been deducted as an 'expense' before arriving at the gross profit.

An important consideration, particularly where companies participate in joint ventures or collaborate on projects, is that if a benefit is determined by the court to have been obtained jointly by co-defendants, the court may make a confiscation order against each defendant for the whole amount of the benefit obtained.[17]

Companies and individuals should also be aware that the prosecutor may ask the court to apply the criminal lifestyle provisions. If the court determines that a defendant has a criminal lifestyle, the consequences can be serious.[18] The lifestyle provisions apply in a number of prescribed circumstances, including where it can

13 *R v. May* [2008] 1 AC 1028.

14 *R v. Waya* [2012] UKSC 51, [2012] 3 WLR 1188, para. 16: courts must consider Article 1 of Protocol 1 of the European Convention on Human Rights (ECHR) when making a confiscation order, and ensure in particular that confiscation is proportionate to the legitimate aim of recovery of the proceeds of crime.

15 *R v. Sale* [2013] EWCA Crim 1306.

16 *R v. Harvey* [2016] 4 All ER 521.

17 *R v. Ahmad and Fields* [2015] AC 299. However, any sum recovered from one defendant must be taken into account when bringing an action against another.

18 s.75, Proceeds of Crime Act 2002 sets out a three-limbed test, namely where the offence in question (1) is specified in Schedule 2 of the Proceeds of Crime Act 2002, (2) constitutes conduct forming part of a course of criminal activity, or (3) was committed over a period of at least six months, and the defendant has benefited from the conduct.

be shown that the conduct in the indictment was committed over at least six months. If one considers an allegation of bribery, this is often charged as both a conspiracy to bribe, as well as a substantive offence of bribery. Typically, a conspiracy charge will involve the offer of a bribe, the award of a contract and then the payments. This may well take much longer than six months, bringing the lifestyle provisions into play for even a simple one-off corrupt payment. If the conditions above are met, it will be assumed that property transferred or expenditure incurred by a corporate defendant over the six years preceding the charge was obtained from general criminal conduct, and is therefore liable to be confiscated, unless the company can show this assumption to be incorrect or that applying the criminal lifestyle provision would risk serious injustice.[19]

Fine 25.4

When considering the extent to which a fine would be appropriate, the court must take into account compensation[20] or confiscation[21] orders made against the offender. Any fine imposed is calculated by reference to the harm caused by the particular criminal conduct. For bribery offences, the appropriate figure is normally the gross profit obtained from the criminal conduct. For fraud offences, it is normally the actual or intended gross gain to the offender, and for money laundering offences, the amount of money laundered.[22]

Once the relevant harm figure is determined, the court will apply a multiplier, to reflect the culpability of the defendant. The Guidelines provide a non-exhaustive list of factors to be taken into account to assess the level of culpability, which will either be high, medium or low. The factors include the role played by the corporate entity in the unlawful activity, the duration of the offence, any obstruction of detection, the scale and vulnerability of the victims, and whether the offence involved the corruption of government officials.[23] The multiplier will either be 300 per cent (high), 200 per cent (medium) or 100 per cent (low). The court will then adjust the percentage within the relevant category range (from 20 per cent up to 400 per cent) depending on any aggravating or mitigating factors, a non-exhaustive list of which is set out in the Guidelines.[24] The fine must represent the seriousness of the offence, as well as the financial circumstances of the defendant.

The court should then 'step back' and consider adjusting the level of the fine based on the effect of compensation, confiscation and fine taken together, which should remove the gain, provide appropriate punishment and act as a deterrent. If a defendant is being sentenced for more than one offence, the court must also consider whether the total sentence imposed on the defendant is just

19 s.10, Proceeds of Crime Act 2002.

20 s.130, Powers of Criminal Courts (Sentencing) Act 2000.

21 ss.6 and 13, Proceeds of Crime Act 2002.

22 The Guidelines, p. 49.

23 Ibid.

24 Ibid., p. 50.

and proportionate based on the misconduct. It is perhaps this step-back element which increases the uncertainty as to the size of fine.

Before the Guidelines were introduced, Lord Justice Thomas stated in relation to the fine element: 'I approach sentencing on the basis in this case that a fine comparable to that imposed in the US would have been the starting point.'[25] This quote was referred to in the first deferred prosecution agreement (DPA).[26] Following that *dictum*, a judge may decide to step back and increase the fine to the level a US court would impose. Anecdotally, we are aware from recent cases that in one instance the judge did enquire of the SFO what the fine would have been if the US Sentencing Guidelines were being followed. Owing to this level of uncertainty and because the fine cannot be agreed by the prosecution and defence even as part of a plea bargain (or DPA), some corporate offenders may wish to consider asking the court for an indication of the sentence it could expect to receive should it plead guilty, often known as seeking a *Goodyear* indication.[27]

The procedure governing such requests is set out in the case of *R v. Goodyear* and the Criminal Practice Directions.[28] If the request is granted, the indication will be confined to the maximum fine the court would impose if the defendant pleaded guilty at that stage in the proceedings. It will not include ancillary matters such as confiscation. The court cannot give an indication where there is a dispute between the parties as to the factual basis for sentencing. The agreed factual basis should be reduced to writing and placed before the judge. Crucially, the judge has absolute discretion to decline to give any indication. If an indication is given and the defendant does not plead guilty having had a reasonable opportunity to consider it, then the indication will fall away. If the case proceeds to trial, the prosecution will not be able to refer to the request for a *Goodyear* indication. A *Goodyear* indication cannot be sought pre-charge and is therefore unlikely to be of assistance in DPA cases.

25.5 Guilty plea

If a guilty plea is entered by the defendant, the court must give the defendant credit.[29] The Reduction in Sentence for a Guilty Plea: Definitive Guideline recommends a sliding scale of discount, which will be applied to the harm figure, dependent on the stage at which the plea is entered: one-third for a plea at the first stage of the proceedings and a maximum of one-quarter thereafter.[30] The

25 *R v. Innospec Ltd*, [2010] Crim LR 665, Southwark Crown Court, 26 May 2010, unreported.

26 *SFO v. Standard Bank Plc* (Case No. U20150854) [2016] Lloyd's Rep FC 102 30 November 2015.

27 See *R v. Goodyear* [2005] 1 WLR 2532.

28 Criminal Practice Directions VII Sentencing C: Indications of Sentence.

29 s.144, Criminal Justice Act 2003.

30 The Reduction in Sentence for a Guilty Plea: Definitive Guideline (https://www.sentencingcouncil.org.uk/publications/item/reduction-in-sentence-for-a-guilty-plea-definitive-guideline-2/) applies, regardless of the date of the offence, to all offenders aged 18 or older and to organisations, where the first hearing in respect of the case is held on or after 1 July 2017. This chapter proceeds on the basis that these guidelines apply.

reduction should be further decreased to a maximum of one-tenth on the first day of trial, having regard to the time when the guilty plea is first indicated relative to the progress of the case and the trial date.[31] The first stage will normally be the first hearing at which a plea or indication of plea is sought and recorded by the court. The Reduction in Sentence for a Guilty Plea: Definitive Guideline explains that where the court is satisfied there were particular circumstances that significantly reduced the defendant's ability to understand what was alleged or otherwise made it unreasonable to enter a guilty plea sooner, a reduction of one-third should still be made. The court should distinguish between cases in which it is necessary to receive advice or see the evidence to understand whether the defendant is guilty of the offence and cases in which a defendant merely delays a guilty plea to assess the strength of the prosecution evidence and the prospects of conviction or acquittal.[32] The court should also consider applying a further discount to reflect any assistance provided by the defendant to the prosecution.[33]

Costs 25.6

The court may make an order in favour of either the prosecution or the defendant.[34] Ordinarily, in the event of a plea or a conviction, the court will make an order that the defendant pay the investigation and court costs of the prosecuting body. If a defendant is acquitted or the prosecution does not proceed to trial, the court may make an order in favour of the defendant. A defendant's costs will be met out of 'central funds' (i.e., public money)[35] in an amount the court considers reasonably sufficient to compensate the defendant for any expenses properly incurred in the proceedings. An award may also be made against a party for unnecessary or improper acts or omissions that result in another party incurring costs.[36] A court may also make an award against a representative (not a party) who conducts litigation in a way that results in wasted costs.[37] A defendant's costs order should usually be made unless there is a positive reason for not doing so.

Private prosecutions are subject to the same costs regime. As a result, while persons who bring a private prosecution without any realistic chance of success will likely be faced with a costs order, they will not generally be liable for costs simply because the prosecution failed or was withdrawn. The justification is that 'the law should guard against inadvertently discouraging the bringing of private prosecutions because of a fear of adverse costs consequences.'[38] A court may also

31 The Reduction in Sentence for a Guilty Plea: Definitive Guideline, Revised June 2017, s.D2.

32 Ibid., s.F1.

33 *R v. Wood* [1992] 2 Cr App R (S) 347.

34 Prosecution of Offences Act 1985; Access to Justice Act 1999; Lord Chief Justice's Practice Direction (Costs in Criminal Proceedings) 201; and Costs in Criminal Case (General) Regulations.

35 s.16, Prosecution of Offences Act 1985.

36 Ibid., at ss.19 and 19A.

37 *Evans v. SFO* [2015] 1 WLR 3595.

38 *The Queen on the Application of David Haigh v. City of Westminster Magistrates' Court* [2017] EWHC 232 (Admin), para. 35.

make an award in favour of a private prosecutor in respect of that party's own costs, to be paid out of central funds, whether or not the defendant is convicted.[39]

25.7 Director disqualifications

Under the Company Directors Disqualification Act 1986 (CDDA), any director convicted of misconduct in connection with a company (either in the United Kingdom or overseas) or considered unfit to be concerned with the management of a company, may be disqualified from the right to manage a company by a disqualification order.[40] A disqualification order may bar a person from acting as a director of any UK company for up to 15 years, and the person will be entered on the register of disqualified directors.

Proceedings for a disqualification order are not brought by the company itself. If a director is convicted of an indictable offence in connection with the promotion, formation or management of a company,[41] usually the court before which the director is convicted will consider whether a disqualification order ought to be made and impose it. The Insolvency Service,[42] however, may look to bring disqualification proceedings before, separately from, or even alongside, a criminal prosecution brought by the SFO or other agency, irrespective of whether the company in question is solvent.

In such instances parties should be wary of competing court timetables and the need to ensure their pleadings are consistent. This is of particular importance because the Insolvency Service may share documents produced to it,[43] and given the wide ambit of any such investigation into the general 'fitness' of an individual to be a director, the production orders issued by the Insolvency Service may be wider than those of another agency. Moreover, the Insolvency Service has a memorandum of understanding with the Financial Reporting Council (FRC),[44] and so it is possible that any such information received is shared on a voluntary basis to the extent 'one regulator considers that information it has gathered will be materially relevant to the other'.[45]

The standard of proof in such proceedings is to the civil standard, but given disqualification involves 'a substantial interference with the freedom of the individual . . . [t]he more serious the allegation, the more the court will need the assistance of cogent evidence'.[46]

---

39 s.17, Prosecution of Offences Act 1985.

40 ss.2(1), 5A(2) and 8(2), CDDA.

41 In addition, any conviction in connection with the liquidation or striking off of a company, with the receivership of a company's propertyor with being an administrative receiver of a company's property may also result in a disqualification order: s.2(1), CDDA.

42 See https://www.gov.uk/government/organisations/insolvency-service.

43 s.447, Companies Act 1985.

44 The Financial Reporting Council (FRC), in turn, has separate memoranda of understanding with the SFO, Financial Conduct Authority and Prudential Regulation Authority.

45 5.2.b, Memoranda of Understanding between the FRC and the Insolvency Service, 18 January 2018.

46 *Re Living Images* [1996] BCC 112, page 116.

In the case of an offence committed outside the United Kingdom, the Secretary of State has standing to apply to the court for a disqualification order, if it appears expedient in the public interest. The Secretary of State also may apply to court for a disqualification order against a person who is (or has been) a director or a shadow director of a company, if it appears expedient in the public interest. On an application, the court may make a disqualification order where it is satisfied that a person's conduct in relation to the company (alone or taken together with their conduct as a director or shadow director of one or more other companies or overseas companies) makes that person unfit to be concerned in the management of a company.

A disqualification order for unfitness may be made on any information properly put before the court that demonstrates that the director or shadow director is unfit to be concerned in the management of a company.[47] As an alternative, the Secretary of State may accept a disqualification undertaking, if it is expedient to do so instead of applying for a disqualification order.

The matters to be taken into account by the court or the Secretary of State, in considering whether a person's conduct makes him or her unfit to be concerned in the management of a company, whether to make a disqualification order and what the period of disqualification should be, are set out in Schedule 1 to the CDDA. Specific matters are to be taken into account where the person is or has been a director, including (1) any misfeasance or breach of fiduciary duty in relation to a company or overseas company, (2) any material breach of any statutory or other obligation that applies as a result of being a director of a company or overseas company, and (3) the frequency of any such conduct.

If a company enters formal insolvency proceedings, the appointed liquidators or administrators must submit reports about directors (including shadow directors) to the Secretary of State if it appears to them the conditions for disqualification are satisfied.[48] For companies entering insolvency proceedings starting on or after 6 April 2016, this obligation to report will apply in respect of all directors and shadow directors (current and past within the previous three years), irrespective of their conduct.[49]

See Chapter 41 on directors' duties

Civil recovery orders 25.8

Companies should also be aware of the SFO's ability to obtain a civil recovery order (CRO) to recover property it has proved, on the balance of probabilities, is or represents property obtained through unlawful conduct, pursuant to Part 5 of the Proceeds of Crime Act 2002 (POCA 2002).

The SFO is not required to obtain a conviction to apply for a CRO. The civil standard of proof and the absence of the need for a conviction have historically made the use of CROs attractive to both the SFO and corporate entities alike.

47 s.109 of the Small Business, Enterprise and Employment Act 2015 removed the previous reference to 'investigative material' in s.8 of the CDDA, with effect from 1 October 2015.

48 s.7, CDDA 1986.

49 s.7A, CDDA 1986.

CROs have also been used by the SFO in addition to a prosecution, to target tainted assets. However, CROs, which are *in rem* actions, have rarely been used by the SFO in this way, as the SFO must show that the property it seeks to recover is the property that has been created by the criminal conduct. Such difficulties associated with proving the exact nature of the property can of course be dealt with by the respondent entity admitting that the property is tainted in the way alleged by the applicant.[50]

One notable case in which the SFO used a CRO to recover tainted assets followed a guilty plea to corruption offences and breaches of UN sanctions in 2009 by the engineering firm Mabey & Johnson Ltd. In 2012, the SFO then successfully obtained a CRO of approximately £130,000 against its parent company, Mabey Engineering (Holdings) Ltd, even though the parent company had no knowledge of the unlawful conduct. The CRO was obtained to recover a sum representing the value of the dividends received by the parent that were derived from contracts won through Mabey & Johnson Ltd's unlawful conduct.

However, the SFO's use of CROs as an alternative to prosecution in corporate matters received considerable criticism, concerning the lack of detail surrounding the underlying criminal conduct, and the basis on which the SFO decided to pursue a CRO rather than a criminal conviction.

Perhaps in light of this criticism, in 2012 the Attorney General's Office published guidance for prosecutors and investigators on how they should use these asset recovery powers.[51] The Attorney General's guidance sets out a non-exhaustive list of circumstances in which these powers might be appropriately used when it is not feasible to secure a conviction. It also sets out a non-exhaustive list of circumstances in which these powers could still be properly used when a conviction is feasible, but the use of asset recovery powers that do not require a conviction might better serve the overall public interest.

The SFO now states that it may use these powers as an alternative (or in addition) to prosecution, but states that if it does so, it will publish its reasons, the details of the illegal conduct and the details of the disposal. In 2018, the SFO obtained a significant CRO (against an individual) following the guilty plea by Griffiths Energy to charges brought by the Canadian authorities for bribing Chadian diplomats to secure contracts. The £4.4 million CRO was brought against the wife of a former Chadian diplomat who received an improper inducement from Griffiths Energy to obtain contracts. The traceable proceeds of this inducement were located in a bank account in London.[52] At the time of writing, the SFO's CRO proceedings against Gulnara Karimova (a daughter of the former

50 As the DPA regime has not been adopted in Scotland, civil recovery remains the route to a negotiated outcome in this jurisdiction.

51 Guidance for prosecutors and investigators on their asset recovery powers under section 2A of the Proceeds of Crime Act 2002, 29 November 2012.

52 *SFO v. Saleh* [2018] EWHC 1012 (QB). For another example of a significant CRO against a corporate, see the 2012 CRO against Oxford Publishing Limited: https://www.sfo.gov.uk/2012/07/03/oxford-publishing-ltd-pay-almost-1-9-million-settlement-admitting-unlawful-conduct-east-african-operations/.

Uzbekistan president Islam Karimov) and Rustam Madumarov continue in connection with alleged corruption in that country.[53] It is as yet unclear what assets the SFO is attempting to seize, or to which deals the assets relate. The SFO has been granted until 3 January 2020 to submit its claim.

Under section 20 of the Criminal Finances Act 2017, the Financial Conduct Authority (FCA) may recover property in cases where there has not been a conviction, but where it can be shown, on the balance of probabilities, that property has been obtained through unlawful conduct. Applications are made in the High Court.

The Criminal Finances Act 2017, Part 1, sections 1 to 9 amends section 362 of POCA 2002 and empowers the High Court to make unexplained wealth orders (UWOs). These require persons suspected of involvement in, or association with, serious criminality to explain the origin of assets that appear to be disproportionate to their known income. A failure to provide a response will give rise to a presumption that the property is recoverable, to assist any subsequent civil recovery action. Persons may also be convicted of an offence if they make false or misleading statements in response to a UWO. Applications can be made by the SFO, NCA and FCA, among others. The NCA secured its first two UWOs in February 2018, against the wife of an individual serving a prison sentence in Azerbaijan for embezzlement, in respect of properties that reportedly cost £22 million. Three further UWOs, in addition to interim freezing orders, were obtained by the NCA in May 2019 in respect of three residential properties in 'prime locations'[54] linked to a politically exposed person believed to be involved in serious crime.

See Chapter 17 on individuals in cross-border proceedings and Chapter 30 on individual penalties

Criminal restraint orders 25.9

The SFO and other enforcement authorities may also apply for a restraint order in the Crown Court. This prevents a defendant from dissipating, disposing of or detrimentally dealing with its assets. The Crown Court may impose a restraint order, which applies to all 'realisable property' currently in the defendant's possession or subsequently acquired by the defendant.[55] As such, restraint orders are the criminal law equivalent of freezing injunctions.

The legislation stipulates five different scenarios in which a restraint order may be imposed.[56] The common thread is that there must normally be reasonable cause to believe that the defendant has benefited from his or her criminal conduct and is likely to dissipate the assets prior to any fine or confiscation order being imposed. If that is the case, an application for a restraint order may be made after commencement of a criminal investigation, during proceedings for an offence,

53 https://www.sfo.gov.uk/2018/10/03/sfo-begins-action-to-recover-proceeds-of-alleged-corrupt-telecoms-deals-in-uzbekistan/.

54 29 May 2019, NCA press release, 'NCA secures Unexplained Wealth Orders for prime London property worth tens of millions'.

55 s.41(2), Proceeds of Crime Act 2002; this is subject to a number of exceptions, such as for legal fees and ordinary living expenses.

56 Ibid., at s.40.

or in the context of specific applications filed by the prosecution. In the event of suspected non-compliance the enforcement authorities may apply to appoint a management receiver[57] or an enforcement receiver,[58] depending on the specific circumstances of the case.

The court has broad discretion in defining the terms of a restraint order,[59] but must require the applicant, usually the SFO or the Crown Prosecution Service (CPS) (which pursues restraint proceedings in cases involving investigations by police or HMRC), to report to the court on the progress of the investigation at specified intervals.[60] A breach of a restraint order constitutes civil contempt.[61]

A considerable challenge presented by restraint orders is that they may prevent individuals or companies from using their funds to obtain legal representation in the proceedings to which the order relates.[62]

25.10 Serious crime prevention orders

Unlike the orders discussed above, Serious Crime Prevention Orders (SCPOs), which were first introduced in the Serious Crime Act 2007 (SCA) and which have been significantly broadened by the Serious Crime Act 2015, can be imposed prior to any finding of criminal liability. SCPOs are civil orders.[63]

SCPOs may be imposed only upon application by the Director of Public Prosecutions (or equivalents in Scotland and Northern Ireland) or the Director of the SFO[64] where the court is satisfied that the person concerned has been involved in 'serious crime' anywhere in the world, and that there are reasonable grounds to believe that an SCPO would protect the public by preventing, restricting or disrupting involvement by the person in serious crime in England and Wales.[65] The CPS will also 'make applications on behalf of other prosecutors for SCPOs' within the Whitehall Prosecutors Group, further to a memorandum of understanding published on 9 October 2017.[66] A recent example of this can be seen when the CPS sought an SCPO on behalf of the FCA in February 2018.[67]

The prosecution needs to prove these matters to the civil standard of proof: namely, it must be more likely than not that the defendant has been involved in serious crime, and that the order would protect the public.[68] However, there is

57 s.48, Proceeds of Crime Act 2002.

58 s.50, Proceeds of Crime Act 2002.

59 Ibid., at s.41(7).

60 Ibid., at s.41(7B)(a).

61 *Director of the Serious Fraud Office v. O'Brien* [2012] EWCA Crim 67.

62 *AP v. CPS* [2008] 1 Cr App R 39.

63 s.35(1), SCA.

64 s.8, SCA. SCPOs are therefore not available in private prosecutions.

65 s.1(1), SCA.

66 Signed by individuals on behalf of the Director of Public Posecutions, the Food Standards Agency, the Insolvency Service, the FCA, Natural Resource Wales, the Environment Agency and the Competition and Markets Authority.

67 Referenced in *R v. Gopee* [2019] EWCA Crim 601.

68 s.35(2), SCA.

authority from the House of Lords regarding antisocial behaviour orders, which are similar to SCPOs in nature and operation, to the effect that the standard of proof in proceedings where 'allegations were made of criminal or quasi-criminal conduct which, if proved, would have serious consequences for the person' is the criminal standard of proof, namely beyond reasonable doubt.[69] It is unclear whether this would apply to SCPOs notwithstanding the statutory provisions, but the CPS has taken the view that the criminal standard does apply to the issue as to whether a defendant was 'involved' in serious crime.[70]

There are two types of SCPO: Crown Court orders and High Court orders. The Crown Court may impose an SCPO only upon conviction of a person for a serious crime. The High Court may make an order without the need for a conviction.[71] The distinction turns on proof of 'involvement in' as opposed to 'conviction of' a serious offence. It follows that 'involvement' is broader than 'conviction', and includes conduct that may have facilitated the commission by another of a serious offence in England and Wales,[72] or that was likely to facilitate such offence, whether or not it was actually committed.[73]

'Serious crime' is defined broadly, and includes any offence listed in Part 1 of Schedule 1 to the SCA, as well as any other offence 'which, in the particular circumstances of the case, the court considers to be sufficiently serious to be treated' as serious crime for the purposes of an SCPO application.[74] Schedule 1 lists an array of specific offences under 16 headings, ranging from trafficking in arms, to substantive money laundering offences, fraud, tax evasion, bribery and offences in relation to breaches of sanctions.[75]

SCPOs may be imposed on individuals as well as bodies corporate, partnerships and unincorporated associations.[76] Where a corporation is in breach of an order, the court may order its dissolution where to do so would be 'just and equitable'.[77] The court has wide discretion in formulating the terms of the SCPO.[78] The overriding test for imposition of an SCPO is that the court may include such terms as

69 *R v. Manchester Crown Court ex p McCann* [2002] UKHL 39, [2003] 1 AC 787.

70 CPS guidance on serious crime prevention orders, available at https://www.cps.gov.uk/legal-guidance/serious-crime-prevention-orders.

71 s.1(1), SCA.

72 s.2(1)(b), SCA.

73 s.2(1)(c), SCA.

74 s.2(2), SCA.

75 Sched. 1, SCA. In particular offences under: Proceeds of Crime Act 2002, ss.327 (concealing, etc. criminal property), 328 (facilitating the acquisition, etc. of criminal property) and 329 (acquisition, use and possession of criminal property); Fraud Act 2006 ss.1 (fraud by false representation, failing to disclose information or abuse of position) and 11 (obtaining services dishonestly); Bribery Act 2010 ss.1 (offences of bribing another person), 2 (offences relating to being bribed) and 6 (bribery of foreign public officials).

76 s.30, SCA.

77 s.27(4)(b), SCA.

78 The court may include a provision allowing a law enforcement agency to enter into a monitoring arrangement with a third-party contractor, and to have the subject of the SCPO pay some of the costs: s.39(4) and (5), SCA.

it considers 'appropriate for the purpose of protecting the public by preventing, restricting or disrupting involvement by the person concerned in serious crime in England and Wales'.[79] Section 5 of the SCA contains a non-exhaustive list of restrictions that might be imposed, such as limitations on financial, property or business dealings;[80] a person's associations or communications;[81] use of any item;[82] and travel both within and outside the jurisdiction.[83] Notably, an SCPO may also include a requirement to provide specified information or disclose documents to law enforcement.[84] While this is subject to legal professional privilege,[85] there is no provision in the SCA to protect the right against self-incrimination. However, a statement made by the defendant in compliance with a request for information may not be given in evidence against the defendant.[86]

The NCA has published a list of all SCPOs in force. In May 2019, 203 were in effect.[87] They have been imposed for a range of offences, ranging from drug trafficking (by far the largest category) to money laundering, illegal immigration and fraud. The conditions imposed in the orders vary in severity, but include restrictions on possessing cash and financial reporting requirements. However, this list does not include SCPOs obtained by local police authorities or HMRC that the NCA was not notified of.

Although at the time of writing there are no publicised examples of SCPOs having yet been used for this purpose, they could allow enforcement authorities to instal monitors in cases involving corporate organisations. To date, monitors have only been appointed in cases involving CROs and DPAs where the corporate organisations have co-operated with enforcement authorities. The SCA provides for the possibility of the appointment of an 'authorised monitor' following conviction regardless of whether the defendant has co-operated during the preceding investigation and proceedings (although there clearly would be significant difficulties associated with appointing a monitor in respect of an unco-operative corporate defendant).

79 s.1(3), SCA (High Court); s.19(5) (Crown Court). Other legislation dealing with civil orders in furtherance of the criminal law, such as ABSOs, sexual offences prevention orders and terrorism prevention and investigation measures impose a requirement of 'necessity' rather than 'appropriateness'. As most applications for an SCPO will engage one or more rights under the ECHR, however, the court will need to consider the Human Rights Act 1998, in particular the precept of proportionality, which includes necessity. See also CPS guidance on serious crime prevention orders (Terms of orders), available at https://www.cps.gov.uk/legal-guidance/serious-crime-prevention-orders.

80 s.5(3)(a), SCA.

81 s.5(3)(c), SCA.

82 s.5(3)e), SCA.

83 s.5(3)(f), SCA.

84 s.5(5)(a), SCA. But a requirement to provide information orally is not permissible: s.11, SCA.

85 s.12, SCA.

86 s.15, SCA. This is similar to the provisions under s.2 of the Criminal Justice Act 1987.

87 See https://nationalcrimeagency.gov.uk/who-we-are/publications/299-nca-ancillary-order-register.

DPAs 25.11

The legislation and DPA Code[88] state that the level of financial penalty imposed as part of a DPA should be broadly comparable to a fine that a court would have imposed following an early guilty plea,[89] which would ordinarily be a reduction of one-third. However, in all but the first DPA[90] approved by the court, a discount of 50 per cent to the financial penalty imposed has been applied. In the *XYZ* DPA (now known to be agreed with Sarclad Limited, following the lifting of reporting restrictions), Sir Brian Leveson, then President of the Queen's Bench Division, considered that a 50 per cent reduction was appropriate as the company had self-reported in a timely way and had fully co-operated with the SFO. The court in its judgment stated that the reduction was made to encourage others to act similarly when confronting corporate criminality.[91] A similar justification also prompted a 50 per cent discount for the *Tesco* DPA[92] and the *Serco* DPA.[93]

In the *Rolls-Royce* DPA, no such initial self-report was made by the company but the court still reduced the financial penalty by 50 per cent. Leveson P cited the following as factors that he took into consideration when reducing the financial penalty: Rolls-Royce's 'extraordinary cooperation' in the SFO's investigation, including voluntary disclosure of internal investigation materials; not winding up companies of interest to the SFO's investigation; and identifying conduct to the SFO that went beyond that which had triggered the SFO's initial investigations.[94]

See Chapter 23 on negotiating global settlements

In addition to a reduced criminal penalty, the mandatory debarment provisions of the Public Contracts Regulations 2015 (the Regulations) will not apply because the entry into a DPA does not constitute a conviction. However, if a DPA is agreed and approved by the court, the DPA and the underlying facts and conduct will be published. A contracting authority (as defined by the Regulations) may consider that the underlying facts and conduct as set out in the DPA are an 'appropriate means' of demonstrating that a company is guilty of 'grave professional misconduct', in accordance with the Regulations, resulting in discretionary debarment from public procurement procedures, as considered below.

Debarment 25.12

In addition to financial penalties, companies will need to be mindful of the impact that any conviction, or misconduct not resulting in a conviction, may have on their ability to tender for public contracts. The rules governing debarment are

88 Deferred Prosecution Agreements Code of Practice; Crime and Courts Act 2013.

89 Crime and Courts Act 2013, Schedule 17, para. 5(4).

90 *Rolls-Royce* [2017] Lloyd's Rep FC 249; *Sarclad Limited* [2016] Lloyd's Rep FC 509; *Tesco Ltd* [2017] 4 WLUK 558; *Serco Geografix Ltd* [2019] 7 WLUK 45.

91 *SFO v. XYZ*, Redacted Approved Judgment (Case No. U20150856), para. 57.

92 In a judgment issued by Leveson P.

93 In a judgment issued by Davies J.

94 *SFO v. Rolls Royce PLC and Rolls Royce Energy Systems Inc*, [2017] Lloyd's Rep FC 249, paras. 16 to 24.

contained in the Regulations, which came into force on 26 February 2015, and which implemented the EU Procurement Directive in the United Kingdom.[95]

Debarment can be mandatory or discretionary. Debarment is mandatory if the tendering company has been convicted of a specific category of offence, including economic crimes such as bribery,[96] corruption, money laundering, fraud or conspiracy to defraud affecting the European Union's financial interests. Debarment will also be mandatory if an individual who is a member of the relevant company's administrative, management or supervisory body, or has powers of representation, decision or control in the company, is convicted of one or more of these offences.[97]

In comparison with the prior legislation, which imposed an automatic, indefinite debarment for companies convicted of these types of offence, mandatory debarment now only applies for a maximum of five years.

Discretionary debarment applies to a different range of conduct, including insolvency, the distortion of competition or where a contracting authority is able to demonstrate by appropriate means that a company is guilty of grave professional misconduct rendering its integrity questionable. A contracting authority may exclude a company from participation in procurement procedures[98] for three years following such conduct.[99]

While the Regulations do not define 'grave professional misconduct', the European Court of Justice has interpreted this term as covering 'all wrongful conduct which has an impact on the professional credibility of the operator'.[100] Reference to a conviction for an economic crime not within the remit of mandatory debarment could form the basis for demonstrating such misconduct.

The most significant change in respect of debarment in the United Kingdom is the introduction of 'self-cleaning', which is applicable to both mandatory and discretionary debarment. The Regulations set out a number of conditions that, if met, can demonstrate a company's suitability for access to public procurement tenders, despite the existence of grounds for mandatory or discretionary debarment. The conditions include the payment of compensation, co-operation with investigative authorities, and the taking of concrete measures to prevent further criminal offences or misconduct being committed. If a contracting authority considers that the evidence of self-cleaning provided to it by a company is sufficient,

95 Directive 2014/24/EU on public procurement.

96 Specifically, the common law offence of bribery; corruption within the meaning of s.1(2) of the Public Bodies Corrupt Practices Act 1889; corruption within the meaning of s.1 of the Prevention of Corruption Act 1906; bribery within the meaning of ss.1, 2 or 6 of the Bribery Act 2010; or bribery within the meaning of s.113 of the Representation of the People Act 1983. The failure of a commercial organisation to prevent bribery, contrary to s.7 of the Bribery Act 2010, will not trigger mandatory debarment but may result in discretionary debarment.

97 Regulation 57(1).

98 Regulation 57(8)(c).

99 Regulation 57(12).

100 Case C-465/11 *Forposta v. Poczta Polska*, para. 27. This was in light of Article 45(2) of the previous Public Procurement Directive, Directive 2004/18/EC, though it remains persuasive in relation to interpretation of the new Public Procurement Directive.

it must not debar the company.[101] The gravity and circumstances of the misconduct are relevant factors when evaluating whether a company has self-cleaned; the graver the offence, the more comprehensive these self-cleaning steps need to be.[102]

Until the *Serco* DPA, there had been no substantive discussion as to what impact a DPA would have in the context of debarment. In the *Serco* DPA, Mr Justice William Davis expressly noted that in his opinion (on the facts of the case) he was satisfied that:

> *[A]pproval of this DPA will not be the determining factor in what is a political decision. Public procurement is subject to statutory regulation, namely by the Public Contracts Regulations 2015. The Regulations provide for mandatory or discretionary debarment in different situations. They also provide for what is known as self-cleaning by which a company can provide that it has taken appropriate remedial action sufficient to satisfy the contracting authority that it has demonstrated its reliability.*[103]

He added: 'The same exercise must follow in the event of the DPA.'[104]

In light of a letter received by William Davis J from the government's Chief Commercial Officer, addressed to the SFO, it was clear that in Serco's case a DPA would not be a mandatory or discretionary bar to contracting with the government. The letter stated that 'we see no current reason why Serco should not continue to be a key strategic supplier to [the UK government]',[105] and, on this basis, William Davis J stated that his 'approval of the DPA, although of relevance, is not the determining factor in terms of Serco PLC or its subsidiaries continuing to provide services to HM Government'.[106] This would appear to also be the case for other companies that have agreed a DPA with the UK government, as on 5 August 2019, when Rolls-Royce announced a contract with the Ministry of Defence to continue to provide support to the Royal Air Force's Typhoon aircraft as 'a follow-on to the 10 year Partnered Support Operational Phase arrangement'.[107]

Regulatory financial penalties and other remedies 25.13

Companies and individuals may also face regulatory sanctions for their misconduct separately and sometimes in addition to any criminal penalties. The primary regulatory authority is the FCA, which regulates firms (such as banks, credit unions and insurance firms) and individuals performing regulated financial services activities. The FCA may bring enforcement action against these firms (as well

101 Regulation 57(13) and 57(14).

102 Regulation 57(16).

103 *Serco Geografix Ltd* [2019] 7 WLUK 45, para. 28.

104 Ibid., at para. 29.

105 Ibid., at para. 30.

106 Ibid.

107 Rolls-Royce press release, 'Rolls-Royce continues to support EJ200 engine for RAF's Typhoon fleet', 5 August 2019.

as individuals) in connection with economic crimes to the extent that it considers there has been a regulatory breach. In certain areas (such as cases concerning market abuse and unauthorised business), it may also take action against persons who are not authorised by it to carry on regulated activities.

On 6 March 2010, the FCA adopted a new method of calculating financial penalties and published the procedure in the Decision Procedure and Penalties Manual (DEPP). This procedure allows the FCA to take into account the revenue generated by the relevant part of the financial institution when determining the level of the fine, which may well be in excess of any gain made through misconduct. In relation to an individual, the FCA will look at the gross amount of any benefit received by the individual in connection with the breach when assessing the fine figure.

The use of the new procedure has resulted in the FCA imposing fines on financial institutions for conduct after 6 March 2010 that are substantially higher than fines that would have been imposed under the previous penalty regime. If the relevant conduct spans the date of both the old and new penalty procedures, the FCA will apply the old procedures to the conduct preceding 6 March 2010 and the new procedures to the subsequent conduct.[108]

Penalty regime after 6 March 2010

Under the penalty regime, the FCA uses five steps to determine the level of a financial penalty it will impose on a firm for a regulatory breach:[109]

1 disgorgement of the financial benefit derived directly from the breach (which may include the profit made or loss avoided);
2 seriousness of the breach;[110]
3 any mitigating and aggravating factors;
4 adjustment for deterrence;[111] and
5 settlement discount.[112]

---

108 We do not consider the penalty regime prior to 6 March 2010 in this chapter, as we anticipate that the number of matters involving conduct that pre-dates March 2010 will likely be small at the time of writing.

109 FCA Handbook, Decision Procedure and Penalties manual (DEPP) 6.5 (current version November 2019).

110 In relation to financial institutions this figure will typically be determined by reference to the 'relevant revenue' from the particular product line or business during the period of the breach. The FCA will determine what percentage of the revenue figure it considers to be an appropriate basis for the financial penalty, from a minimum of 0 per cent to a maximum of 20 per cent. The assessment is based on a number of factors including the impact and nature of the breach, and whether the breach was deliberate or reckless. A Level 5 breach is most serious at 20 per cent of relevant revenue, reducing in 5 per cent increments, such that a Level 1 breach is 0 per cent. The figure to be imposed under this section is in addition to the disgorgement amount.

111 If the FCA considers the figure arrived at after Step 3 is insufficient to deter the firm that committed the breach, or others, from committing further or similar breaches, the FCA may increase the financial penalty.

112 If the financial institution settles all issues of fact and liability at the earliest stage, it will receive a 30 per cent reduction on the financial penalty. However, this will not apply to any disgorgement sum due.

Since the introduction of this regime, the FCA has an increased flexibility in determining the level of financial penalty to imposed on a financial institution. For any misconduct after 6 March 2010, the penalty regime gives the FCA wide discretion in determining the 'relevant revenue' forming the basis for the penalty, and this can now include the underlying revenue of the relevant part of the financial institution. However, the FCA may consider other factors when considering the seriousness of the breach, such as market capitalisation, where 'relevant revenue' is not deemed to be an appropriate measure of the harm caused by the breach.[113]

After the introduction of the revised DEPP, there was a marked increase in the fines imposed by the FCA (or its predecessor) from just over £66 million in 2011 to nearly £1.5 billion in 2014.[114] However, in 2018 the FCA levied fines totalling just under £60.5 million.[115] It is the authors' view that the introduction of the revised DEPP happened to coincide with a period of increased regulatory enforcement activity, for example in connection with the benchmark manipulation and foreign exchange manipulation cases, which resulted in an unusual spike in financial penalties, rather than the spike being attributable solely to the revisions to DEPP.

On 1 March 2017, the FCA introduced a new enforcement procedure for disciplinary cases.

Under this procedure, four options are available to parties looking to resolve cases at an early stage in proceedings. These are:

- obtain a 30 per cent discount on the penalty if the firm or individual settles both the factual issues, the fact of a regulatory breach and the amount of penalty with the FCA;
- obtain a 30 per cent discount if the firm or individual agrees with the FCA all the relevant facts and accepts that they amount to regulatory breaches, whether or not the firm or individual disputes the penalty to be imposed;
- obtain a 15 to 30 per cent discount if the firm or individual agrees with the FCA all the relevant facts but disputes that they amount to regulatory breaches and disputes the penalty. The percentage of the discount made available to the firm or individual is at the discretion of the Regulatory Decisions Committee (RDC), the decision-making board responsible for deciding if enforcement action is appropriate; or
- obtain a 0 to 30 per cent discount in penalty if the firm or individual partly agrees with the FCA some of the facts, liability and penalty, but disputes a narrow set of issues. Again, the percentage of the discount made available to the firm or individual is at the discretion of the RDC.[116]

113 https://www.fca.org.uk/publication/final-notices/tejoori-limited-2017.pdf, paras. 6.5 to 6.11; https://www.fca.org.uk/publication/decision-notices/cathay-international-holdings-limited-2019.pdf, section 6.

114 http://www.fca.org.uk/firms/being-regulated/enforcement/fines.

115 https://www.fca.org.uk/news/news-stories/2018-fines.

116 https://www.fca.org.uk/publication/corporate/enforcement-information-guide.pdf.

As a result, settlement discounts will now be available in a wider range of circumstances allowing regulated firms to challenge aspects of the FCA's enforcement team's findings before the RDC.[117]

25.14 Withdrawing a firm's authorisation

In addition to imposing financial penalties on authorised firms and individuals, the FCA has a number of other powers at its disposal to meet its strategic and operational objectives, in particular ensuring that financial markets function well, protecting consumers and ensuring integrity and competition in the markets.[118] Perhaps the most draconian measure the FCA can impose on a firm is the withdrawal of its authorisation to engage in regulated activities.

The Financial Services and Markets Act 2000 (FSMA), as substantially revised by the Financial Services Act 2012, imposes a general prohibition on a person or entity engaging in 'regulated activities', which are defined in Schedule 2 to FSMA, but include most financial advisory and transactional work.[119] The general prohibition applies unless a person, legal or natural, is exempt or has been 'authorised' to engage in such activity under FSMA.[120] A common form of such authorisation is permission given by the FCA to a firm under Part 4A of FSMA. In granting permission, the FCA must ensure that the authorised person is satisfying certain 'threshold conditions', and will continue to do so. One key threshold condition is suitability: an authorised person must be 'a fit and proper person having regard to all the circumstances'.[121] The FCA's powers include a right to cancel this permission if it appears to the FCA that the authorised person is failing or is likely to fail to fulfil the threshold conditions.[122]

The withdrawal power is exercisable where the FCA believes that it is 'desirable to exercise the power to advance one or more of its operational objectives'.[123] While the power is broadly worded, the FCA's Enforcement Guidelines state that the cancellation power will be exercised mainly where the FCA has 'very serious concerns' about a firm, or the way its business is or has been conducted.[124] More specifically, this will be the case where the firm has repeatedly failed to comply

117 See, e.g., *Linear Investments Limited v. Financial Conduct Authority* [2019] UKUT 0115 (TCC) https://assets.publishing.service.gov.uk/media/5cac6ef3e5274a42a5619fcf/Linear__Investements_Ltd_v_FCA.pdf. Linear Investments Limited entered into a focused resolution agreement with the FCA, by which is agreed matters of fact and liability with the FCA. However, it disputed the FCA's proposed penalty of £409,300 and appealed to the Upper Tribunal, in the first case of its kind. The Upper Tribunal confirmed the amount of the penalty.

118 s.1B(1) to (3), FSMA.

119 Sched. 2, FSMA.

120 s.19, FSMA.

121 Sched. 6, para. 2E, FSMA. Other threshold conditions relate to matters such as office location, effective supervision, resources and business model.

122 s.55J(1)(a), FSMA. The FCA may also cancel permission if the authorised person has not engaged in regulated activity in the previous 12 months: s.55J(1)(b).

123 s.55J(1)(c), FSMA.

124 EG 8.5.1, FCA.

with FCA rules and requirements, or has failed to co-operate with the FCA to the extent that it is no longer satisfied that the firm is fit and proper.[125] Withdrawal of permission means that the person ceases to be authorised and cannot engage in any regulated activities.[126] As an alternative to withdrawing permission, the FCA has broad powers to vary a Part 4A permission, or to impose specific conditions on its exercise instead.[127]

Senior Managers and Certification Regime 25.15

Both the Senior Managers and Certification Regime (SMCR) and the Approved Persons Regime regulate individuals exercising functions on behalf of regulated entities. At the time of writing, the SMCR applies to UK banks, building societies, credit unions, Prudential Regulatory Authority-designated investment firms, branches of foreign banks operating in the United Kingdom, and insurance and reinsurance firms. In December 2019, the SMCR will be extended to apply to all firms authorised under FSMA. We only consider the SMCR in this chapter.

The SMCR contains the following three elements:

- *Senior Managers Regime*: This applies to all individuals performing Senior Management Functions (SMF). These individuals need to be approved by the FCA or PRA as appropriate.
- *Certification Regime*: This applies to all employees of regulated firms who could pose a risk of significant harm to the firm or its customers. These individuals are not approved by the FCA or PRA; rather, the employing firm must certify (both at the outset of employment and on a continuing basis) that the individual is fit and proper to carry out his or her functions.
- *Conduct Rules*: Both the FCA and the PRA have issued high-level requirements that apply to individuals falling within the ambit of the SMCR. These replace the Statements of Principle and Code of Practice for Approved Persons. In practice, the FCA Conduct Rules apply to all employees of the FCA, except those performing ancillary functions (for example, receptionists and post room staff). They apply to almost all staff of FCA authorised firms in the United Kingdom, and to those staff based outside the United Kingdom who deal with UK customers.

Section 59ZA of FSMA defines SMF as follows:

> *A function is a 'senior management function', in relation to the carrying on of a regulated activity by an authorised person, if – (a) the function will require the person performing it to be responsible for managing one or more aspects of the authorised person's affairs, so far as relating to the activity, and (b) those aspects involve, or might involve, a risk of serious consequences (i) for the authorised person, or (ii) for business or other interests in the United Kingdom.*

125 EG 8.5.2(7) and (8), FCA.
126 ss.19 and 31(1)(a), FSMA.
127 ss.55J and 55L, FSMA.

The FCA has designated a number of particular positions within firms as being SMFs (including some 'catch-all' functions designed to cover firms' particular arrangements). Not all of these positions will be applicable in every authorised firm. The FCA and PRA have also specified over 30 prescribed responsibilities within authorised firms (again, not all will apply in every case). These responsibilities, if applicable, must be formally assigned to an SMF within the firm. The individuals holding those positions are then accountable for the proper performance of those responsibilities, and applications for approval to the FCA and PRA must be accompanied by corresponding statements of responsibility.

The FCA and the PRA can take enforcement action against senior managers if:

- the manager is responsible for any activities in the firm in relation to which the firm contravenes a regulatory requirement; and
- the manager has not taken such steps as a person in his or her position could reasonably be expected to take to avoid the contravention occurring (or continuing).

The regulators therefore must prove a contravention of a regulatory requirement by the firm, in an area for which the senior manager was responsible. The burden of proof is on the regulators.

The designation of SMF does not necessarily entail an increase in personal liability from that which existed prior to the introduction of the SMCR; it enables the FCA and the PRA to more effectively identify those individuals responsible for areas of firms in which there has been a breach. Senior managers remain liable for being knowingly concerned with breaches by firms of relevant rules, and the FCA and PRA can take enforcement action against senior managers and certified individuals for breaches of the Conduct Rules.[128]

25.16 Restitution orders

The FCA may also seek restitution where it seeks to compensate those adversely affected by a breach of regulatory provisions.

The FCA will take the following considerations into account in determining whether to seek restitution, in the light of 'all the circumstances of the case': whether the profits are quantifiable or the losses identifiable; the number of persons affected; costs to the FCA; alternative redress, such as compensation schemes or another regulator; whether victims can be expected to bring proceedings in their own right; the firm's solvency; alternative powers available to the FCA; and the conduct of persons having suffered loss, for example whether they have contributed to their loss.[129] This list is not exhaustive. The FCA can apply to court for restitution, and if it finds that these requirements are met, the court may order payment of a sum it considers 'just' having regard to the profits made or loss

128 Only FCA Conduct Rules 1 to 5 apply to certified persons or other employees falling within scope; all of the FCA's Conduct Rules apply to senior managers. Only PRA Conduct Rules 1 to 3 apply to certified persons.

129 EG 11.2.1, FCE.

caused.[130] If the court orders restitution, the money will be paid to the FCA rather than to the person who has suffered loss or at whose expense a profit has been made (FSMA refers to these as 'qualifying persons').[131] However, the FCA must then disburse the money among the qualifying persons according to the terms of the court order.[132] The payment of restitution does not bar an ancillary civil claim for damages being brought by qualifying persons.[133]

See Chapter 33 on parallel civil litigation

Where appropriate, the FCA will consider imposing a restitution order using its administrative powers.[134] A restitution order may be imposed where the FCA is 'satisfied that a person has contravened a relevant requirement, or been knowingly concerned in the contravention of such a requirement'.[135] Further, the person against whom the order is sought must either have profited from the contravention, or must have caused loss or an otherwise adverse effect to another.[136] The FCA will usually choose to apply to the court (rather than using its administrative powers) for a restitution order where there is another factor requiring the involvement of the court. For example, where there is a risk of dissipation, a need to combine the restitution order with a separate order or a concern that the individual subject to the order may not comply.

On 28 March 2017, the FCA used its powers[137] for the first time to require a listed company to pay compensation for market abuse. Tesco agreed that it committed market abuse in relation to a trading update it published on 29 August 2014, which gave a false or misleading impression regarding the value of publicly traded Tesco shares and bonds. Tesco agreed to pay compensation to investors who purchased Tesco securities on or after 29 August 2014 and who still held those securities when the statement was corrected on 22 September 2014. Under the compensation scheme, Tesco must pay each investor an amount equal to the inflated price of each security. The FCA estimated that the total compensation payable under the scheme was likely to be in the region of £85 million, plus interest.[138]

The Office of Financial Sanctions Implementation 25.17

In the past year the Office of Financial Sanctions Implementation (OFSI) issued its first-ever financial penalties for breaches relating to financial sanctions, following the introduction of powers in the Policing and Crime Act 2017 (PCA17) aiming to strengthen the government's ability to punish financial sanctions breaches. The

130 s.382(2), FSMA.

131 Ibid.

132 s.382(3), FSMA.

133 s.382(7), FSMA.

134 s.384, FSMA.

135 s.382(1) and (6), FSMA. The meaning of 'relevant requirement' is somewhat narrower than under the injunction provisions, but is substantially the same; see s.382(9).

136 Ibid.

137 s.384, FSMA.

138 https://www.fca.org.uk/news/press-releases/tesco-pay-redress-market-abuse.

penalties, imposed against Raphael & Sons plc for £5,000[139] and Travelex UK Ltd for £10,000,[140] both relate to violations of the EU–Egypt financial sanctions regime.

The maximum penalty that OFSI can impose for a financial sanctions is £1 million or, where the breach relates to particular funds or resources with an estimable value, 50 per cent of the estimated value of the funds or resources – whichever is greater.[141] The PCA17 also raised the maximum term of imprisonment for financial sanctions offences to seven years[142] and amended the DPA regime such that financial sanctions breaches are now included in the list of offences for which a DPA may be entered into.[143]

25.18 The Information Commissioner's Office

The Information Commissioner's Office (ICO) may issue fines and prosecute individuals and corporates it considers have engaged in criminal activity in respect of their data protection obligations. At the time of writing, the ICO has engaged in 12 prosecutions where monetary penalties were sought, and one prosecution where the individual in question was sentenced to six months in prison.[144]

The ICO has, however, been more active in issuing civil monetary penalties, with 54 monetary penalties since 24 November 2017.[145] Following the implementation of the General Data Protection Regulation (GDPR) in the United Kingdom via the Data Protection Act 2018 (DPA 2018), the ICO has issued two intention-to-fine notices under that legislation, which significantly increases the maximum penalties for breaches of data protection law from £500,000[146] to €10 million or 2 per cent of worldwide turnover (whichever is greater)[147] or €20 million or 4 per cent of worldwide turnover (whichever is greater)[148] depending on the nature of the breach.

The notices were issued against British Airways[149] and Marriott International[150] for personal data breaches affecting data subjects within the European Union.

139 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804117/190502_Raphaels_revised_notice.pdf.

140 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804021/Travelex_monetary_penalty.pdf.

141 s.146, PCA17.

142 Ibid., at s.144.

143 Ibid., at s.150, inserting para. 26A into Part 2 of Schedule 17 to the Crime and Courts Act 2013.

144 https://ico.org.uk/action-weve-taken/enforcement/?facet_type=Prosecutions&facet_sector=&facet_date=&date_from=&date_to=.

145 https://ico.org.uk/action-weve-taken/enforcement/?facet_type=Monetary+penalties&facet_sector=&facet_date=&date_from=&date_to=.

146 Data Protection Act 1998 s.55A as prescribed by section 2 of The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010.

147 GDPR, Article 83(4), as implemented by s.157, DPA 2018.

148 GDPR, Article 83(5), as implemented by s.157, DPA 2018.

149 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

150 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

These proposed fines, of approximately £183 million and £99 million respectively, if issued without reduction following the written representation and appeal processes, indicate that the risks associated with compliance with data protection law have become significantly higher following the implementation of the GDPR. Given that the United Kingdom has incorporated the GDPR into its national law via the DPA 2018, this position is unlikely to change following its departure from the European Union.

Disclosure to other authorities 25.19

A look at recent enforcement action shows that UK enforcement authorities co-operate with a number of other enforcement authorities around the world, particularly in the United States. Such co-operation may be governed by legislation, a memorandum of understanding, or less formally through information sharing gateways.

It is therefore possible that, if a company or individual is found criminally liable or in breach of its regulatory obligations in the United Kingdom, the details of the offence or regulatory breach will be made known to interested enforcement authorities in other jurisdictions. If the company or individual faces liability in those jurisdictions, disclosure by the United Kingdom authorities may lead to further enforcement action. This issue naturally should be considered prior to a company or individual accepting any criminal or regulatory liability or entering into an agreement with enforcement authorities. Further, the SFO has made it clear in its Corporate Co-operation Guidance[151] that where a company seeks to co-operate with the SFO, the SFO expects to be notified in the event that any other government agencies contact the company, or if the company reports to any other government agencies.[152]

See Chapter 3 on self-reporting and Chapter 11 on production to authorities

Even if a company is not facing criminal or regulatory liability in other jurisdictions, it will still need to establish whether the local legal requirements would require a disclosure of a finding of criminal liability and subsequent financial penalty. Whether a disclosure is required will depend on the jurisdiction in which the company operates. If there is no local legal requirement to make a disclosure, foreign enforcement authorities may still expect to be notified of any finding of liability and subsequent financial penalty. Whether a voluntary disclosure is made will turn on what is expected by the local regulator and the implications of disclosure or non-disclosure. Such decisions are complicated by issues regarding personal data, which should be considered whenever it is transferring across jurisdictions to disclose misconduct to other enforcement agencies.

See Chapter 40 on data protection

151 SFO Operational Handbook, Corporate Co-operation Guidance, available at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/.

152 Ibid.

26

Fines, Disgorgement, Injunctions, Debarment: The US Perspective

Gayle E Littleton, Charles D Riely, Amanda L Azarian and Grace C Signorelli-Cassady[1]

26.1 Introduction

This chapter considers the potential fines, penalties and other collateral consequences that corporates may face in the United States when defending against, or settling an enforcement action with, US regulators.

The US enforcement authorities have a variety of means to seek redress from corporates and individuals, including financial penalties and equitable remedies. The general purpose and policy objectives behind the sanctions are (1) to deter the defendant and others from committing such offences in the future, (2) to protect the public, (3) to punish the defendant and (4) to promote rehabilitation of the defendant.[2] In considering fines and penalties, the US enforcement authorities and courts will consider the facts and circumstances of the matter, including whether the defendant accepts responsibility for the conduct, any remediation that has been effected and co-operation by the defendant with the relevant enforcement authorities.[3]

See Chapter 10 on co-operating with authorities

In recent years, both the Department of Justice (DOJ) and Securities and Exchange Commission (SEC) have been successful in extracting significant financial penalties as part of their enforcement actions and settlements.[4] In the fiscal

1 Gayle E Littleton and Charles D Riely are partners, and Amanda L Azarian and Grace C Signorelli-Cassady are associates, at Jenner & Block LLP. The authors also wish to acknowledge the contribution of Rita D Mitchell of Wilkie Farr & Gallagher, the original author of the chapter in previous editions on which this chapter is partly based.

2 See, e.g., Department of Justice, Justice Manual § 9-27.110.

3 See, e.g., Department of Justice, Justice Manual § 9-27.420.

4 For example, in 2014, BNP Paribas agreed to plead guilty and pay US$8.9 billion for alleged violations of US economic sanctions in Iran, Sudan and Cuba, of which US$140 million was a fine and US$8.8336 billion was forfeiture. (Department of Justice press release, 'BNP Paribas

year ending 30 September 2015, DOJ collected a total of US$23.1 billion in civil and criminal penalties; in 2016, the combined figure was approximately US$15.3 billion.[5] The SEC obtained orders totalling approximately US$16 billion in disgorgement and penalties for fiscal years 2015 to 2018.[6]

While DOJ has recently emphasised the importance of prosecuting individuals rather than corporates and announced a new policy seeking to 'discourage disproportionate enforcement of laws by multiple authorities', it is too soon to tell whether these policy shifts will lead to a decrease in the total monetary fines and penalties collected.[7] In May 2018, it rolled out a policy to 'avoid the unnecessary

---

Agrees to Plead Guilty and to Pay $8.9 Billion for Illegally Processing Financial Transactions for Countries Subject to U.S. Economic Sanctions' (30 June 2014), available at https://www.justice.gov/opa/pr/bnp-paribas-agrees-plead-guilty-and-pay-89-billion-illegally-processing-financial.) In 2016, VimpelCom reached an approximately US$800 million resolution with the US and Dutch authorities over allegations of bribery of an Uzbek government official, of which US$230 million was a criminal penalty to the Department of Justice (DOJ), US$167.5 million was disgorgement and prejudgment interest to the Securities and Exchange Commission (SEC), and US$397.5 million was paid to Dutch prosecutors as a criminal penalty. (Department of Justice press release, 'VimpelCom Limited and Unitel LLC Enter into Global Foreign Bribery Resolution of More Than $795 Million; United States Seeks $850 Million Forfeiture in Corrupt Proceeds of Bribery Scheme' (18 February 2016), available at https://www.justice.gov/opa/pr/vimpelcom-limited-and-unitel-llc-enter-global-foreign-bribery-resolution-more-795-million.) In a related action, which has been stayed until 31 January 2020, DOJ is also seeking US$850 million in forfeiture of the corrupt proceeds of the alleged scheme (*United States of America v. All Funds Held in Account Number CH1408760000050335300*, 1:16-cv-01257, (S.D.N.Y.) Docket No. 34). In 2018, Société Générale agreed to pay over US$1 billion to US and French authorities to resolve charges relating to bribery of officials in Libya and manipulation of the London Inter-Bank Offered Rate, of which US$860 million was in criminal penalties and US$475 million was in regulatory penalties and disgorgement. (Department of Justice press release, 'Société Générale S.A. Agrees to Pay $860 Million in Criminal Penalties for Bribing Gaddafi-Era Libyan Officials and Manipulating LIBOR Rate' (4 June 2018), available at https://www.justice.gov/opa/pr/soci-t-g-n-rale-sa-agrees-pay-860-million-criminal-penalties-bribing-gaddafi-era-libyan.) In March 2019, a Russian telecommunications company, Mobile TeleSystems PJSC (MTS), settled Foreign Corrupt Practices Act (FCPA) violations with the SEC and DOJ for a total of US$850 million, none of which will be paid to non-US enforcement authorities. (Department of Justice press release, 'Mobile Telesystems Pjsc and Its Uzbek Subsidiary Enter Into Resolutions of $850 Million with the Department of Justice for Paying Bribes In Uzbekistan' (7 March 2019), available at https://www.justice.gov/opa/pr/mobile-telesystems-pjsc-and-its-uzbek-subsidiary-enter-resolutions-850-million-department.)

5 Department of Justice press release, 'Justice Department Collects More Than $23 Billion in Civil and Criminal Cases in Fiscal Year 2015' (3 December 2015), available at https://www.justice.gov/opa/pr/justice-department-collects-more-23-billion-civil-and-criminal-cases-fiscal-year-2015; Department of Justice press release, 'Justice Department Collects More Than $15.3 Billion in Civil and Criminal Cases in Fiscal Year 2016' (14 December 2016), available at https://www.justice.gov/opa/pr/justice-department-collects-more-153-billion-civil-and-criminal-cases-fiscal-year-2016.

6 Securities and Exchange Commission, Division of Enforcement Annual Report (2 November 2018), available at https://www.sec.gov/files/enforcement-annual-report-2018.pdf.

7 Department of Justice News, 'Deputy Attorney General Rod Rosenstein Delivers Remarks to the New York City Bar White Collar Crime Institute' (9 May 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

imposition of duplicative fines, penalties, and/or forfeiture' against a corporate being investigated by multiple enforcement authorities.[8] The policy requires DOJ lawyers from all departments to coordinate internally and, when possible, with 'other federal, state, local, or foreign enforcement authorities' to curb the practice of 'piling on' fines and penalties, 'with the goal of achieving an equitable result'.[9] Regardless, in an active enforcement environment, corporates and individuals who are facing enforcement action should be mindful of the potential consequences and the opportunities to manage and reduce the ultimate fines and penalties.

See Chapter 24 on negotiating global settlements

26.2 Standard criminal fines and penalties available under federal law

26.2.1 Maximum financial penalties

Many federal statutes contain their own fining provisions, which typically include a maximum fine amount. Additionally, for some crimes, the Alternative Fines Act provides for an alternative maximum fine of double the gross gain (or gross loss caused to another) from the unlawful activity.[10] Where a fine is imposed against an officer, director, employee, agent or shareholder of an issuer, the fine may not be paid, directly or indirectly, by the issuer.[11]

In addition, for certain offences, DOJ may seek criminal or civil forfeiture, or both, of property that constitutes, or is derived from proceeds traceable to, the offence.[12] Recent examples of forfeiture include (1) DOJ complaints against

8 Department of Justice, Justice Manual § 1-12.100 – Coordination of Corporate Resolution Penalties in parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (May 2018).

9 The policy sets out various factors that should be considered when coordinating between multiple DOJ units or enforcement authorities, including 'the egregiousness of a company's misconduct; statutory mandates regarding penalties, fines, and/or forfeitures; the risk of unwarranted delay in achieving a final resolution; and the adequacy and timeliness of a company's disclosures and its cooperation with the Department, separate from any such disclosures and cooperation with other relevant enforcement authorities'. (Department of Justice, Justice Manual § 1-12.100 – Coordination of Corporate Resolution Penalties in parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (May 2018).) A recent example of this policy in action can be found in the Department's March 2019 US$850 million settlement with MTS and related SEC settlement carrying a civil penalty of US$100 million. According to a press release: 'Consistent with Coordination of Corporate Resolution Penalties in Parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (Justice Manual 1-12.100), the Department of Justice agreed to credit the civil penalty paid to the SEC as part of its agreement with MTS. Thus, the combined total amount of criminal and regulatory penalties paid by MTS and [its subsidiary] to U.S. authorities will be $850 million.' (Department of Justice press release, 'Mobile Telesystems Pjsc and Its Uzbek Subsidiary Enter Into Resolutions of $850 Million with the Department of Justice for Paying Bribes In Uzbekistan' (7 March 2019), available at https://www.justice.gov/opa/pr/mobile-telesystems-pjsc-and-its-uzbek-subsidiary-enter-resolutions-850-million-department.)

10 See 18 U.S.C. § 3571; *Southern Union Co. v. United States*, 132 S.Ct. 2344, 2350-52 (2012).

11 15 U.S.C. § 78ff(c)(3).

12 See, e.g., 18 U.S.C. § 982(a) (in connection with sentencing persons convicted of certain federal offences, including money laundering and other financial crimes, courts shall order criminal forfeiture of property 'involved in such offense, or any property traceable to such property');

various officials and associates of the sovereign wealth fund, 1MDB, in connection with allegations of an international conspiracy to launder misappropriated funds, seeking civil forfeiture totalling approximately US$1.7 billion[13] and (2) the US Attorney's Office for the District of Nevada obtaining a forfeiture order from the District Court requiring the former president and chief executive officer of MRI International, found guilty on multiple counts of mail and wire fraud and money laundering in connection with a Ponzi scheme, to pay US$813 million.[14]

Defendants may also be required to pay restitution, taking into consideration the amount of loss sustained by each victim, the financial resources of the defendant and any other factors the court deems appropriate.[15]

On 8 October 2019, DOJ issued a non-binding policy memorandum to Criminal Division attorneys that provides 'guidance and an analytical framework' on evaluating a company's ability to pay a criminal fine or criminal monetary

18 U.S.C. § 981(a) (property involved in certain federal offences, including money laundering and other financial crimes, 'or any property traceable to such property', is subject to civil forfeiture). Under civil forfeiture statute 18 U.S.C. § 981(a)(1)(C), property relating to a 'specified unlawful activity' as defined in 18 U.S.C. § 1956(c)(7) is subject to civil forfeiture. Among the 'specified unlawful activities' listed in 18 U.S.C. § 1956(c)(7) are racketeering, bribery of a public official, fraud by or against a foreign bank, export control violations and violations of the FCPA. Further, 28 U.S.C. § 2461(c) 'permits the government to seek *criminal* forfeiture whenever civil forfeiture is available *and* the defendant is found guilty of the offense'. *United States v. Newman*, 659 F.3d 1235, 1239 (9th Cir. 2011) (original emphasis).

13 Department of Justice press release, 'U.S. Seeks to Recover Approximately $38 Million Allegedly Obtained from Corruption Involving Malaysian Sovereign Wealth Fund' (22 February 2019), available at https://www.justice.gov/opa/pr/us-seeks-recover-approximately-38-million-allegedly-obtained-corruption-involving-malaysian.

14 Department of Justice press release, 'President And CEO Of Las Vegas Investment Company Sentenced to 50 Years in Prison for Running $1.5 Billion Ponzi Scheme' (23 May 2019), available at https://www.justice.gov/opa/pr/president-and-ceo-las-vegas-investment-company-sentenced-50-years-prison-running-15-billion.

15 18 U.S.C. § 3663(a)(1)(B)(i). See, e.g., *United States v. Savoie*, 985 F.2d 612, 619 (1st Cir. 1993) (holding civil settlement did not bar defendant, convicted of racketeering violations, of having to pay restitution of US$93,476.67, as restitution 'is not a civil affair; it is a criminal penalty meant to have deterrent and rehabilitative effects'). In *Kelly v. Robinson*, the Supreme Court commented on restitution as follows: 'The criminal justice system is not operated primarily for the benefit of victims, but for the benefit of society as a whole. Thus, it is concerned not only with punishing the offender, but also with rehabilitating him. Although restitution does resemble a judgment "for the benefit of" the victim, the context in which it is imposed undermines that conclusion. The victim has no control over the amount of restitution awarded or over the decision to award restitution. Moreover, the decision to impose restitution generally does not turn on the victim's injury, but on the penal goals of the State and the situation of the defendant. As the Bankruptcy Judge who decided this case noted in *Pellegrino*: "Unlike an obligation which arises out of a contractual, statutory or common law duty, here the obligation is rooted in the traditional responsibility of a state to protect its citizens by enforcing its criminal statutes and to rehabilitate an offender by imposing a criminal sanction intended for that purpose".' 479 U.S. 36, 52, 107 S. Ct. 353, 362, 93 L. Ed. 2d 216 (1986).

penalty when inability to pay is claimed.[16] The memo sets forth various legal considerations and relevant factors that should be taken into account if legitimate questions remain after an analysis of an inability-to-pay questionnaire. These factors include background on current financial position, alternative sources of capital, collateral consequences and victim restitution considerations.

26.2.2 United States Sentencing Guidelines

Federal courts in the United States use the United States Sentencing Guidelines (the Sentencing Guidelines) as guidance in considering the aggravating and mitigating circumstances of a crime and imposing a sentence. These apply to both corporates and individuals. Although district courts must consult the Sentencing Guidelines and take them into account, they are not required to apply them.[17] A recent study, in fact, suggests that federal trial judges 'now follow the advisory fraud guideline range in less than half of all cases', providing for sentences 'well below the fraud guideline'.[18]

For corporates, the calculation of the applicable fine is made by (1) identifying a 'base fine',[19] (2) identifying the minimum and maximum multipliers that combined with the base fine create a 'fine range'[20] and (3) considering potential 'departures', upwards or downwards, from the fine range.[21]

In calculating the base fine under the Sentencing Guidelines, the first step is to identify the 'offence level', which depends on the characteristics of the crime. The 'base offence level' is set according to the nature of the conduct or the statute violated, and then the overall offence level will increase or decrease depending on certain factors.[22] For example, for an anti-bribery violation under the Foreign Corrupt Practices Act (FCPA), the base offence level is 12.[23] Factors that may affect the overall offence level include the number of bribes, the dollar amount involved and the position of the foreign official receiving the payment or benefit.[24] The total offence level helps to determine the base fine, which is the greatest of the amount specified in a table that translates the offence level into a base fine, the

16 Department of Justice, Criminal Division, Memorandum on Evaluating a Business Organization's Inability to Pay a Criminal Fine or Criminal Monetary Penalty (8 October 2019), https://www.justice.gov/opa/speech/file/1207576/download.

17 The Sentencing Guidelines were mandatory until the Supreme Court's decision in *United States v. Booker*, 543 U.S. 220, 125 S.Ct. 738, 160 L.Ed.2d 621 (2005).

18 Mark Bennett, Justin Levinson and Koichi Hioki, 'Judging Federal White-Collar Fraud Sentencing: An Empirical Study Revealing the Need for Further Reform', *Iowa Law Review*, 989, Vol. 102:939 (2017); George Pierpoint, 'Is white-collar crime treated more leniently In the US?', BBC News (11 March 2019), available at https://www.bbc.co.uk/news/world-us-canada-47477754.

19 United States Sentencing Commission, Guidelines Manual, § 8C2.4.

20 United States Sentencing Commission, Guidelines Manual, §§ 8C2.6, 8C2.7.

21 United States Sentencing Commission, Guidelines Manual §§ 8C4.1-8C4.11.

22 Base offence levels are set out in Chapter Two of the Guidelines Manual.

23 United States Sentencing Commission, Guidelines Manual § 2C1.1.

24 United States Sentencing Commission, Guidelines Manual §§ 2C1.1(b)(1)-(3).

pecuniary gain to the organisation from the offence, or the pecuniary loss from the offence caused by the organisation, 'to the extent the loss was caused intentionally, knowingly, or recklessly'.[25]

The second step is to calculate the 'culpability score', which yields the minimum and maximum multipliers to be applied to the base fine. The culpability score is based on the characteristics of the defendant. Relevant factors may include the size of the organisation and the degree of participation in, or tolerance of, the wrongdoing; the defendant's prior criminal history; whether the defendant has violated an order or injunction, or violated a condition of probation by committing similar misconduct to that for which probation was ordered; obstruction of justice; the existence of an effective compliance programme; and self-reporting, co-operation and acceptance of responsibility.[26] The potential multipliers can range from 0.05 (a reduction of 20 times the base fine) to 4.0 (four times the base fine), depending on the culpability score. The fine range reflects the minimum and maximum multipliers as applied to the base fine. In addition to the fine, any gain to the corporate from an offence that is not otherwise part of the corporate's restitution or remediation is subject to disgorgement.[27]

Finally, the Sentencing Guidelines allow for upward or downward departures from the fine range. This may include a downward departure for substantial assistance to the government in its investigation of others[28] or remedial costs that exceed the gain to the corporate.[29] Unlike the factors that are considered for calculating the offence level and culpability score, the detriments or benefits that result from departures are not quantified. The court in its discretion imposes a fine within the fine range, or above or below the range by taking into account any departures. For negotiated resolutions, a corporate through its counsel will often negotiate and agree to a downward departure recommendation beyond the low end of the fine range.

Civil penalties 26.3

Civil monetary sanctions can include penalties, disgorgement and prejudgment interest. Each of these has a different purpose and method of calculation.

The SEC may impose civil monetary penalties on any person who violates or causes a violation of the securities laws. The Securities Act of 1933 and the Securities Exchange Act of 1934 authorise three tiers of civil penalties. Less serious civil violations fall into the first tier, where the penalty is no more than US$9,472 for an individual or US$94,713 for a corporate for 'each act or omission' violating the federal securities laws. The second tier applies to violations involving fraud, deceit, manipulation, or deliberate or reckless disregard of a regulatory requirement, for which the maximum penalty is US$94,713 for individuals

25 United States Sentencing Commission, Guidelines Manual § 8C2.4.
26 United States Sentencing Commission, Guidelines Manual § 8C2.5.
27 United States Sentencing Commission, Guidelines Manual § 8C2.9.
28 United States Sentencing Commission, Guidelines Manual § 8C4.1.
29 United States Sentencing Commission, Guidelines Manual § 8C4.9.

and US$473,566 for corporates, again for each act or omission. Finally, the third tier applies to violations involving fraud, deceit, manipulation, or deliberate or reckless disregard of a regulatory requirement that also directly or indirectly resulted in 'substantial losses . . . to other persons' or 'substantial pecuniary gain to the person who committed the act or omission'.[30] Third-tier penalties have a limit of US$189,427 for individuals and US$947,130 for corporates, for each act or omission.[31] Civil penalties for insider trading depend on the amount of the profits generated by the illicit trading. A district court can order civil penalties up to three times the profit gained or loss avoided by the violative trade.[32]

DOJ likewise may seek civil penalties in certain types of matters, such as violations of federal financial, health, safety, civil rights and environmental laws.[33] For example, the Royal Bank of Scotland agreed to pay a US$4.9 billion civil penalty under the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 for its involvement in a scheme that misled investors and failed to disclose significant risks about its residential mortgage-backed securities ultimately contributing to the 2008 financial crisis.[34]

26.4 Disgorgement and prejudgment interest

The SEC may also seek disgorgement to prevent an entity or individual from profiting from illegal conduct and to deter subsequent misconduct.[35] Disgorgement has often accounted for a significant portion of the overall enforcement sanction. For example, in March 2019, Fresenius Medical Care agreed to pay the SEC and DOJ more than US$231 million to settle allegations that it had violated the FCPA, of which US$147 million (the full amount imposed by the SEC and 63 per cent of the total) was disgorgement.[36] Disgorgement can also be sought

30 15 U.S.C. § 78u-2(b); 17 C.F.R. § 201.1001 and Securities and Exchange Commission, 'Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission (as of 15 January 2019)', available at https://www.sec.gov/enforce/civil-penalties-inflation-adjustments.htm (effective 15 January 2019). The maximum civil penalty amounts noted above are for violations after 2 November 2015. Maximum civil penalty amounts will be adjusted annually for inflation, as described in 17 C.F.R. § 201.1001.

31 Id.

32 15 U.S.C. § 78u-1(a).

33 See, e.g., 12 U.S.C. § 1833a (providing a civil money penalty provision to the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 which allows DOJ to seek civil penalties against persons who violate one of 14 enumerated statutes); 42 U.S.C. § 3614(d)(1)(C) (allowing it to seek civil penalties for violations of the Fair Housing Act of 1968).

34 Department of Justice press release, 'Royal Bank of Scotland Agrees to Pay $4.9 Billion for Financial Crisis-Era Misconduct: Settlement Is Largest Penalty Imposed On A Single Entity By The Justice Department For Financial Crisis-Era Misconduct' (14 August 2018), available at https://www.justice.gov/opa/pr/royal-bank-scotland-agrees-pay-49-billion-financial-crisis-era-misconduct.

35 See *SEC v. Huffman*, 996 F.2d 800, 802 (5th Cir. 1993); *SEC v. Cavanaugh*, 445 F.3d 105, 117 (2d Cir. 2006) (noting that disgorgement 'has the effect of deterring subsequent fraud').

36 Department of Justice press release, 'Fresenius Medical Care Agrees to Pay $231 Million in Criminal Penalties and Disgorgement to Resolve Foreign Corrupt Practices Act Charges' (29 March 2019), available at https://www.justice.gov/opa/pr/fresenius-medical-care-agrees-pay-231-million-criminal-penalties-and-disgorgement-resolve; Securities and Exchange Commission

in certain circumstances even when DOJ declines to prosecute the corporate under its Corporate Enforcement Policy. For example, it declined to prosecute Cognizant Technology Solutions for violations of the FCPA, yet the company agreed to pay nearly US$20 million in disgorgement, which represented 'all profits fairly attributable to the bribery conduct'.[37]

The SEC's ability to extract large disgorgement payments has been recently limited by a decision issued by the United States Supreme Court that held that the typical five-year limitation period applying to any 'action, suit or proceeding for the enforcement of any civil fine, penalty, or forfeiture, pecuniary or otherwise' applies to disgorgement.[38] The SEC had previously taken the position, and some Circuit Courts had held, that disgorgement was an equitable remedy[39] and that the SEC was therefore not constrained by any limitation period when seeking disgorgement. On 5 June 2017, however, the US Supreme Court unanimously rejected the SEC's position in *Kokesh v. SEC*, holding that '[d]isgorgement in the securities-enforcement context is a "penalty" . . . and so disgorgement actions must be commenced within five years of the date the claim accrues'.[40] In so doing, the Supreme Court resolved a Circuit split.[41]

There will be a substantial impact on the amount the SEC is able to recover in certain cases. In *Kokesh v. SEC*, for example, the District Court had ordered the defendant to pay US$34.9 million in disgorgement, of which US$29.9 million

press release, 'SEC Charges Medical Device Company With FCPA Violations' (29 March 2019), available at https://www.sec.gov/news/press-release/2019-48.

37 Department of Justice Declination Letter, 'Re: Cognizant Technology Solutions Corporation' (13 February 2019), available at https://www.justice.gov/criminal-fraud/file/1132666/download.

38 28 U.S.C. § 2462; *Kokesh v. SEC*, 137 S. Ct. 1635 (2017).

39 *Kokesh v. SEC*, 137 S.Ct. 1635, 1640-41 (2017); *SEC v. Contorinis,* 743 F.3d 296, 306-07 (2d Cir. 2014) ('[W]hile both criminal forfeiture and disgorgement serve to deprive wrongdoers of their illicit gain, the two remedies reflect different characteristics and purposes – disgorgement is an equitable remedy that prevents unjust enrichment, and criminal forfeiture a statutory legal penalty imposed as punishment. . . . Moreover, unlike disgorgement, which is a discretionary, equitable remedy, criminal forfeiture is mandatory and a creature of statute. Thus, unlike the criminal forfeiture case, the district court's discretion in determining disgorgement is not confined by precise contours of statutory language, but rather serves the broader purposes of equity.').

40 *Kokesh v. SEC*, 137 S.Ct. 1635, 1639 (2017).

41 *Compare SEC v. Graham*, 823 F.3d 1357, 1363-64 (11th Cir. 2016) (holding that § 2462's statute of limitations applies to disgorgement) with *SEC v. Kokesh*, 834 F.3d 1158, 1164-67 (10th Cir. 2016) (holding that the disgorgement sought was neither a penalty nor a forfeiture under § 2462) and *Riordan v. SEC*, 627 F.3d 1230, 1234 (D.C. Cir. 2011) (holding that disgorgement is not a 'civil penalty' and therefore not subject to the five-year statute of limitations); *SEC v. Tambone*, 550 F.3d 106, 148 (1st Cir. 2008) ('[T]he applicable five-year statute of limitations period [the defendant] invokes applies only to penalties sought by the SEC, not its request for injunctive relief or the disgorgement of ill-gotten gains.'), reinstated in relevant part, 597 F.3d 436, 450 (1st Cir. 2010).

related to conduct outside the limitation period and is therefore now time-barred.[42] As of the 2018 fiscal year end, the SEC estimated that it could 'forgo up to approximately $900 million' in pending cases due to the ruling.[43]

Since *Kokesh v. SEC* was decided, defendants have further sought to rely on the decision to challenge the SEC's statutory authority for seeking disgorgement at all, arguing that, as a penalty, disgorgement is not within the court's equitable powers. Although some courts have been receptive to such challenges,[44] many have construed *Kokesh* narrowly.[45] On 1 November 2019, the Supreme Court granted *certiorari* in *Liu v. SEC*, No. 18-501, to consider whether the SEC can seek disgorgement in actions filed in federal courts.[46] If the Supreme Court determines that the SEC lacks the power to seek disgorgement in such cases, this could curtail the agency's ability to demand significant monetary sanctions in future actions.

The calculation of disgorgement involves quantifying the amount of profits obtained as a result of the illegal conduct and can be complex. Given the challenges in distinguishing between legally and illegally derived profits, in considering the amount to be disgorged, courts have broad discretion and need only consider a 'reasonable approximation of profits causally connected to the violation'.[47] Disgorgement amounts may include both 'direct pecuniary benefit[s]' and 'illicit benefits . . . that are indirect or intangible'.[48] Once the SEC meets its burden of

42 *Kokesh v. SEC*, 137 S.Ct. 1635, 1641 (2017).

43 Securities and Exchange Commission, Division of Enforcement Annual Report (2 November 2018), available at https://www.sec.gov/files/enforcement-annual-report-2018.pdf.

44 *United States v. Latorella*, 2017 WL 2785413, at *4, n. 4 (D. Mass. 27 June 2017), appeal dismissed *sub nom., United States v. Fields*, 2017 WL 6945887 (1st Cir. 19 December 2017). ('It bears noting that [in *Kokesh v. SEC*,] the Supreme Court earlier this month expressly reserved the question "whether courts possess authority to order disgorgement in SEC enforcement proceedings".'); *Osborn v. Griffin*, 865 F.3d 417, 470 n. 1 (6th Cir. 2017) (Merritt, J dissenting) (stating that the theory of 'equitable disgorgement' 'may not even be applicable in SEC contexts for much longer in light of the Supreme Court's' *Kokesh* decision); *SEC v. Arcturus Corp.*, No. 3:13-CV-4861-K, 2018 WL 1701998, at *2 (N.D. Tex. 10 January 2018) ('The Fifth Circuit has repeatedly stated that district courts enjoy "broad discretion" in ordering disgorgement. Unless, and until, current binding authority changes, this Court understands its authority to order disgorgement in SEC proceedings such as this.') (citation omitted).

45 See, e.g., *SEC v. Jammin Java Corp.*, 2017 WL 4286180, at *3 (C.D. Cal. 14 September 2017) (rejecting defendant's contention that 'because the imposition of a penalty is not within the Courts' traditional equity powers, *Kokesh* should be construed so as to eliminate the disgorgement remedy altogether').

46 See, *Liu v. Securities and Exchange Commission*, SCOTUSblog, https://www.scotusblog.com/case-files/cases/liu-v-securities-and-exchange-commission/.

47 See, e.g., *SEC v. Contorinis*, 743 F.3d 296, 304-5 (2d Cir. 2014) (noting that disgorgement must be a 'reasonable approximation of profits causally connected to the violation') (quoting *SEC v. Patel*, 61 F.3d 137, 139-40 (2d Cir. 1995); *Allstate Insurance Co. v. Receivable Finance Co., LLC,* 501 F.3d 398, 413 (5th Cir. 2007) (citing *SEC v. First City*, 890 F.2d 1215, 1231 (D.C. Cir. 1989)); *SEC v. Global Express Capital Real Estate Investment Fund*, I, LLC, 289 Fed. Appx. 183, 190 (9th Cir. 2008); *SEC v. Warren*, 534 F.3d 1368, 1370 (11th Cir. 2008).

48 *SEC v. Contorinis*, 743 F.3d 296, 306 (2d Cir. 2014).

establishing a reasonable approximation of profits causally connected to the fraud, the burden shifts to the defendant to demonstrate that the gains were not affected by the offence.[49] The final decision rests with the court.

Defendants face significant challenges in trying to reduce disgorgement amounts or carve out certain categories of costs and expenses. Although revenue received from improper conduct may be disgorged, it is less clear whether and how the costs associated with that revenue would be used to reduce the disgorgement amount. Several courts have permitted defendants to deduct expenses that are directly associated with the revenue to be disgorged.[50] On the other hand, courts have generally refused to allow defendants to deduct overhead costs or general business expenses from disgorgement amounts on the basis that they were not directly related to the illegal conduct at issue and would have been incurred irrespective of the conduct.[51] By way of example, courts have denied requests to deduct from revenue expenses related to employees' salaries,[52] capital gains taxes paid in connection with illicit profits[53] and fees paid to clearing agents that could not be directly tied to the illegal sales.[54] As a consequence, 'SEC disgorgement sometimes exceeds the profits gained as a result of the violation'.[55]

Because disgorgement was not generally viewed as a 'fine' or 'penalty' until the Supreme Court's *Kokesh* decision, practitioners had also considered the possibility that an FCPA disgorgement payment might be tax-deductible. As a general matter, Internal Revenue Service (IRS) regulations preclude a tax deduction for penalties and fines paid to government authorities, on the basis that taxpayers should not be permitted to enjoy a tax benefit based on a payment designed to be punitive.[56] However, the Tax Code does not specifically address disgorgement. On 6 May 2016, the Office of the Chief Counsel of the Internal Revenue Service released an advice memorandum stating that the disgorgement payment to the SEC in a corporate FCPA action was not tax-deductible, on the basis that a disgorgement amount would, in its view, fall within Section 162(f) of the Tax Code stating that deductions are not allowed 'for any fine or similar penalty paid

49 *SEC v. Razmilovic*, 738 F.3d 14, 32-33 (2d Cir. 2013).

50 *SEC v. McCaskey*, 2002 WL 850001 at *4 (S.D.N.Y. 26 March 2002) (noting that a court may deduct any 'direct transaction costs' such as brokerage commissions from the disgorgement amount); *SEC v. Shah*, 1993 WL 288285 at *5 (S.D.N.Y. 28 July 1993) (allowing defendant to deduct the commissions paid to his broker to effectuate trades based on inside information). But see *F.T.C. v. Bronson Partners, LLC*, 654 F.3d 359, 375 (2d Cir. 2011) ('it is well established that defendants in a disgorgement action are "not entitled to deduct costs associated with committing their illegal acts"') (quoting *SEC v. Cavanagh*, 2004 WL 1594818 at *30 (S.D.N.Y. 16 July 2004), aff'd, 445 F.3d 105 (2d Cir. 2006).

51 *SEC v. Svoboda*, 409 F. Supp. 2d 331, 345 (S.D.N.Y. 2006); *SEC v. Great Lakes Equities Co.*, 775 F. Supp. 211, 215 (E.D. Mich. 1991). ('[T]here is no basis for deducting the costs of fixed expenses since those expenses would be incurred whether or not the fraud took place.')

52 *SEC v. Benson*, 657 F. Supp. 1122, 1134 (S.D.N.Y. 1987).

53 *SEC v. Svoboda*, 409 F. Supp. 2d 331, 345 (S.D.N.Y. 2006).

54 *SEC v. Zwick*, 2007 WL 831812 at *23 (S.D.N.Y. 16 March 2007).

55 *Kokesh v. SEC*, 137 S. Ct. 1635, 1644 (2017).

56 26 C.F.R. § 1.162-21.

to a government for the violation of any law'.[57] Following *Kokesh*, the Office of the Chief Counsel of the Internal Revenue Service reaffirmed this position in an advice memorandum of 1 December 2017, noting that because 'as the Supreme Court held, disgorgement payments are penalties and are not compensatory, section 162(f) prohibits a deduction . . . for an amount paid as disgorgement for violating a federal securities law'.[58] Although these internal memoranda are not binding, they reflect the position of the IRS on this matter.

The SEC also generally obtains prejudgment interest on any disgorgement amount. The rules that apply to administrative proceedings cases brought by the SEC require that such amounts be included in any disgorgement.[59] District courts presiding over actions generally may determine whether prejudgment interest is appropriate.[60] The interest rate applied is typically the 'underpayment' rate set by the IRS.[61] There is no single approach for measuring when the clock begins to run on interest calculations. In some cases, it has been measured from the date the ill-gotten funds were received, up to the date of judgment.[62] In others, it may run from multiple dates where the matter involves multiple transactions,[63] or, where the applicable dates are difficult to identify, from the date of the complaint.[64]

---

57 See https://www.irs.gov/pub/irs-wd/201619008.pdf.

58 See https://www.irs.gov/pub/irs-wd/201748008.pdf.

59 17 C.F.R. § 201.600(a). In recent years, the SEC has increasingly sought to use administrative proceedings rather than federal court proceedings to enforce the federal securities laws. In 2012, for example, there were nearly twice as many administrative proceedings as civil actions brought by the Commission. See Sonia Steinway, 'SEC "Monetary Penalties Speak Very Loudly," But What Do They Say? A Critical Analysis of the SEC's New Enforcement Approach', *Yale Law Journal*, 124:209 (2014). The increased use of administrative proceedings has led to widespread criticism of the Commission around unfairness as well as constitutional challenges around due process. In September 2015, the SEC proposed amendments to the Rules of Practice governing its internal administrative proceedings, which were adopted in July 2016. These amendments, however, do not fully address the concerns that have been raised and challenges to the use of administrative proceedings continue.

60 *SEC v. First Jersey Sec., Inc.*, 101 F.3d 1450, 1476 (2d Cir. 1996).

61 Id., 101 F.3d at 1476 (citing SEC Rules and Regulations, 60 Fed. Reg. 32738, 32788 (23 June 1995)). See also 17 C.F.R. § 201.600(b). The underpayment rate charged by the IRS is three percentage points above the federal short-term rate and for purposes of calculating interest on sums disgorged is compounded quarterly. 26 U.S.C. § 6621(a)(2); 17 C.F.R. § 201.600(b).

62 *SEC v. DiBella*, 2008 WL 6965807 at *3 (D. Conn. 18 July 2008); *SEC v. GMC Holding Corp.*, 2009 WL 506872 at *6 (M.D. Fla. 27 February 2009) ('The time frame for the imposition of prejudgment interest usually begins with the date of the unlawful gain and ends at the entry of judgment.') (quoting *SEC v. Yun*, 148 F. Supp. 2d 1287, 1293 (M.D. Fla. 2001).

63 S*EC v. Savino*, 2006 WL 375074 at *18 & n.10 (S.D.N.Y. 16 February 2006) (calculating interest from the first day of the month following each improper trade).

64 *SEC v. United Energy Partners, Inc.*, 2003 WL 223392 at *2 n.12 (N.D. Tex. 28 January 2003), aff'd, 88 F. App'x 744 (5th Cir. 2004) (using date of complaint for accrual of prejudgment interest award where dates on which defendant acquired disgorged funds were not clear); *SEC v. GMC Holding Corp.*, 2009 WL 506872 at *6 (M.D. Fla. 27 February 2009) (same).

Injunctions 26.5

DOJ may also seek affirmative relief through an injunction where it is deemed necessary to advance public interests or enforce government functions. Such injunction actions may be specifically provided for by statute, may be used to enforce statutes that do not specifically provide for injunctive relief or may be sought from an appellate court pursuant to the All Writs Act.[65]

Likewise, the SEC may seek either a preliminary or permanent injunction when it appears that a person is engaged in, or is about to engage in, acts or practices constituting a violation of the securities laws.[66]

Other consequences 26.6

In addition to the criminal and civil penalties noted above, defendants may face other consequences as a result of a US criminal or civil action. For one, defendants may also face civil and criminal forfeiture of assets, including real and personal property constituting, or derived from proceeds traceable to, a violation, or to a conspiracy to commit a violation.[67] For certain offences, courts are required to order that property traceable to an offence be forfeited.[68]

See Chapter 18 on individuals in cross-border proceedings and Chapter 31 on individual penalties

Further, investigation or prosecution by authorities in one jurisdiction may also lead to investigations, prosecutions or resolution short of prosecution by authorities in other jurisdictions. For example, in recent years two international telecommunications companies, Stockholm-based Telia Company and Amsterdam-based VimpelCom Limited, entered into global resolutions to resolve investigations by the SEC, DOJ and Dutch authorities, agreeing to pay nearly US$1 billion and US$800 million in criminal and regulatory penalties, respectively.[69] It is expected that this trend of multinational investigations and co-operation across jurisdictions will continue in the coming years.

See Chapter 24 on negotiating global settlements

Defendants may also face a variety of actions from other US government agencies, international organisations, other corporates or even shareholders and employees, actions which may involve additional litigation and other monetary penalties.

65 28 U.S.C. § 1651(a). See US Department of Justice Civil Resource Manual, 'Injunctions', available at https://www.justice.gov/jm/civil-resource-manual-214-injunctions.

66 15 U.S.C. § 77t(b); 15 U.S.C. § 78u(d).

67 See 18 U.S.C. §§ 981, 982; 28 U.S.C. § 2461.

68 See 18 U.S.C. § 982.

69 See Department of Justice press release, 'Telia Company AB and Its Uzbek Subsidiary Enter Into a Global Foreign Bribery Resolution of More Than $965 Million for Corrupt Payments in Uzbekistan' (21 September 2017), available at https://www.justice.gov/opa/pr/telia-company-ab-and-its-uzbek-subsidiary-enter-global-foreign-bribery-resolution-more-965; Department of Justice press release, 'VimpelCom Limited and Unitel LLC Enter into Global Foreign Bribery Resolution of More Than $795 Million; United States Seeks $850 Million Forfeiture in Corrupt Proceeds of Bribery Scheme' (18 February 2016), available at https://www.justice.gov/opa/pr/vimpelcom-limited-and-unitel-llc-enter-global-foreign-bribery-resolution-more-795-million.

See Chapter 32 on monitorships

In addition, in connection with certain types of enforcement actions, such as FCPA enforcement, money laundering and sanctions violations, corporates may also be required to retain corporate compliance monitors. For example, in June 2019, Walmart entered into a three-year non-prosecution agreement pursuant to which it agreed not only to pay a combined penalty of US$137 million but also to retain an independent corporate compliance monitor for two years to resolve the government's FCPA investigation.[70]

Finally, in some circumstances, individuals or entities may be barred or suspended from doing business with the executive branch of the United States government.[71] Debarment may be triggered by a criminal conviction or, in some circumstances, even an adverse civil judgment, and applies to all subdivisions of a corporation unless the decision is limited by its terms to specific divisions or organisational units.[72] Suspension may occur upon adequate evidence that certain wrongdoing was committed and when it is in the public's interest.[73] Like debarment, suspension affects all organisational divisions of a corporation, unless otherwise specified.[74]

26.7 Financial penalties (and prison terms) under specific statutes

By way of example, the fines, penalties and other sanctions associated with particular federal criminal statutes of potential interest are outlined below.

26.7.1 Foreign Corrupt Practices Act

The FCPA criminalises bribery of foreign officials, either directly or through an intermediary, to obtain business or some other benefit. Its anti-bribery provisions apply not only to all US corporates and persons, but also can apply to foreign corporates that issue securities within the United States or file certain reports with the SEC (issuers) and to these issuers' officers and employees, among others. The FCPA also criminalises actions taken in the United States by foreign corporates or their agents that are in furtherance of an improper payment or offer. Further, the FCPA's books and records and internal controls provisions also require corporates whose securities are listed in the United States or who file reports with the SEC to keep accounting records that accurately reflect the corporate's transactions and to maintain a system of internal controls.[75]

70 See Department of Justice press release, 'Walmart Inc. and Brazil-Based Subsidiary Agree to Pay $137 Million to Resolve Foreign Corrupt Practices Act Case' (20 June 2019), available at https://www.justice.gov/opa/pr/walmart-inc-and-brazil-based-subsidiary-agree-pay-137-million-resolve-foreign-corrupt.

71 48 C.F.R. §§ 9.406-1(c), 9.407-1(d).

72 48 C.F.R. §§ 9.406-1(b), 9.406-2(a).

73 48 C.F.R. §§ 9.407-1(a), 9.407-2(a).

74 48 C.F.R. § 9.407-1(c).

75 15 U.S.C. §§ 78dd-1(a), 78dd-2(a), 78dd-3(a), 78(m).

Violations of the FCPA can result in heavy penalties. For one, corporate entities may be subject to financial penalties of up to US$2 million per violation of the FCPA's anti-bribery provisions,[76] US$25 million per violation of the FCPA's accounting provisions,[77] or up to twice the gross pecuniary gain or loss from the violation pursuant to the Alternative Fines Act.[78] In addition, civil penalties for FCPA anti-bribery and accounting provisions violations may apply.[79]

Further, certain individuals may be either fined up to US$100,000 (US$250,000 under the Alternative Fines Act or twice the gain or loss from the violation) or imprisoned for up to five years, or both, for a criminal violation of the FCPA's anti-bribery provisions.[80] For criminal violations of the FCPA's accounting provisions, certain individuals can be subject to a fine of up to US$5 million or imprisonment for up to 20 years, or both.[81] Individuals may also face civil penalties for FCPA anti-bribery and accounting provisions violations.[82] Issuers, as defined under the FCPA, are prohibited from paying these individuals' criminal and civil fines.[83]

Moreover, DOJ may also bring a civil action to seek an injunction against domestic concerns and persons other than issuers to prevent a current or imminent FCPA violation.[84] Likewise, the SEC may also seek injunctions to prevent FCPA violations from occurring.[85]

In addition, disgorgement is often a key component of a civil resolution of the FCPA. By way of example, in April 2018, Dun & Bradstreet agreed to pay more than US$9 million to resolve FCPA charges alleging that two Chinese subsidiaries made improper payments to Chinese government officials and third parties to benefit the business, and then falsely recorded these payments as legitimate business expenses. Of the total amount paid by Dun & Bradstreet (more than US$9 million), more than US$6 million was disgorgement.[86]

76 15 U.S.C. §§ 78dd-2(g)(1)(A), 78 dd-3(e)(1)(A), 78ff(c)(1)(A).

77 15 U.S.C. § 78ff(a).

78 18 U.S.C. § 3571 (c)(2), (d).

79 15 U.S.C. §§ 78ff(c)(1)(B), 78u(d)(3); 17 C.F.R. § 201.1001; Securities and Exchange Commission, 'Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission (as of January 15, 2019)', available at https://www.sec.gov/enforce/civil-penalties-inflation-adjustments.htm.

80 15 U.S.C. §§ 78dd-2(g)(2), 78dd-3(e)(2); 18 U.S.C. § 3571 (b)(2), (b)(3), (d).

81 15 U.S.C. § 78ff(a).

82 15 U.S.C. §§ 78ff(c)(2)(B), 78u(d)(3); 17 C.F.R. § 201.1001; Securities and Exchange Commission, 'Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission (as of January 15, 2019)', available at https://www.sec.gov/enforce/civil-penalties-inflation-adjustments.htm.

83 15 U.S.C. § 78ff(c)(3).

84 15 U.S.C. §§ 78dd-2(d), 78dd-3(d).

85 15 U.S.C. § 78u(d)(1).

86 Securities and Exchange Commission press release, 'SEC Charges Dun & Bradstreet With FCPA Violations' (23 April 2018), available at https://www.sec.gov/enforce/34-83088-s.

However, for corporates seeking to avoid the heaviest penalties, the FCPA Corporate Enforcement Policy establishes a presumption that, 'absent aggravating circumstances' such as involvement by executive management in the misconduct or significant profit to the corporate from the misconduct, a corporate will receive a declination if it 'has voluntarily self-disclosed misconduct in an FCPA matter, fully cooperated, and timely and appropriately remediated'. Moreover, even if aggravating circumstances are present, for a corporate that voluntarily self-discloses, fully co-operates and timely and appropriately remediates, DOJ will still recommend a 50 per cent reduction off the low end of the US Sentencing Guidelines fine range, except in the case of a recidivist.[87]

Recently, on 20 November 2019, the FCPA Corporate Enforcement Policy was amended to clarify that a corporate that voluntarily discloses misconduct need not disclose 'all relevant facts known to it', but simply 'all relevant facts known to it at the time of the disclosure'. In addition, the new policy explains that, for a corporate to fully co-operate, it must identify 'relevant evidence not in the company's possession' that the corporate is aware of.[88] However, the corporate is no longer required to identify opportunities 'to obtain relevant evidence not in the company's possession and not otherwise known to the Department' that the corporate 'is or should be aware of'.[89]

26.7.2 Federal criminal money laundering

The principal federal criminal money laundering statues are 18 USC Sections 1956 and 1957. Section 1956 generally prohibits a person who knows that property represents the proceeds of certain unlawful activities from engaging in financial transactions that either promote further unlawful activity, conceal the proceeds, evade taxes or avoid reporting requirements. Section 1957 also prohibits a person from knowingly engaging in a monetary transaction involving property valued at more than US$10,000 that derives from specified unlawful activities. In regards to both sections, the specified unlawful activities include proceeds resulting from offences involving bribery of a foreign official.[90]

See Chapter 18 on individuals in cross-border proceedings and Chapter 31 on individual penalties

Any violation of Section 1956 is punishable by imprisonment for not more than 20 years, a fine of up to US$500,000 or twice the value of the property involved, or both. In addition, such violations can incur a civil penalty up to the greater of US$10,000 or the value of the property involved in the offence, plus asset forfeiture. For Section 1957, the maximum penalty is 10 years' imprisonment or a fine of up to twice the value of the property involved, or both.[91]

87 Department of Justice, FCPA Corporate Enforcement Policy, available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.

88 Id.

89 Department of Justice, FCPA Corporate Enforcement Policy (updated March 2019), available at https://www.justice.gov/criminal-fraud/file/838416/download.

90 18 U.S.C. §§ 1956, 1957.

91 Id.

Export controls and trade sanctions 26.7.3

The US Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces most US economic sanctions. However, the US Commerce Department's Bureau of Industry and Security and DOJ National Security Division also enforce some aspects of US sanctions. Generally, these sanctions, such as the blocking of assets and trade restrictions, are used to accomplish national security and foreign policy objectives.

The sanctions can be either comprehensive for a jurisdiction, such as Cuba,[92] or targeted to particular individuals and entities, such as the sanctions imposed on specific Hezbollah officials in July 2019.[93] Typically, US sanctions either restrict activities that take place in the US or restrict activities that involve a 'US person', generally defined widely to include US citizens, permanent residents, persons present in the United States, and corporates organised under the laws of the United States or any jurisdiction therein, as well as those corporates' foreign branches.[94] However, non-US persons and corporates can face penalties under US sanctions as well, including for 'causing' a violation by a US person.[95] For example, in 2017, OFAC entered into a settlement with CSE TransTel, a subsidiary of a Singapore-based corporate, in part for causing US financial institutions to engage in prohibited conduct involving Iran.[96]

Fines for violations of the sanctions regulations can be significant. As of 10 July 2019, OFAC had settled 18 enforcement actions, with civil penalties totalling more than US$1.2 billion.[97] Criminal penalties for wilful violations of OFAC sanctions can include fines ranging up to US$1 million per violation or imprisonment of up to 20 years, or both.[98] Under Title 18, Section 3571, the government can also pursue fines and penalties against an organisation of up to US$500,000 or twice the pecuniary gain or loss derived from the offence, as well as forfeiture under 18 USC Section 981. Further, penalties for violations of the Trading with the Enemy Act, which provides the statutory authority for the Cuba sanctions, can be up to US$89,170 per violation (which may be adjusted for inflation), and criminal penalties can reach US$1 million.[99] Financial penal-

92 Continuation of the Exercise of Certain Authorities Under the Trading With the Enemy Act, 83 Fed. Reg. 46347 (10 September 2018).

93 Department of the Treasury, 'Treasury Targets Iranian-Backed Hizballah Officials for Exploiting Lebanon's Political and Financial System' (9 July 2019), available at https://home.treasury.gov/news/press-releases/sm724.

94 See, e.g., 31 C.F.R. §§ 560.312, 560.314.

95 See, e.g., 50 U.S.C. § 1705(a).

96 Department of the Treasury, 'Settlement Agreement' (July 2017), available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/transtel_settlement.pdf.

97 Department of the Treasury, '2019 Enforcement Information', available at https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx.

98 See, e.g., 50 U.S.C. § 1705(c).

99 31 C.F.R. § 501.701; Continuation of the Exercise of Certain Authorities Under the Trading With the Enemy Act, 83 Fed. Reg. 46347 (10 September 2018) (extending the expiration of Cuba sanctions pursuant to the Trading with the Enemy Act until September 2019).

ties for violations of the International Emergency Economic Powers Act, which underlies other sanctions programmes, are also possible; associated civil penalties can be up to US$250,000 or twice the amount of the unlawful transaction, and criminal penalties permit a fine of up to US$1 million and imprisonment of up to 20 years.[100]

26.7.4 Racketeer Influenced and Corrupt Organizations Act

The Racketeer Influenced and Corrupt Organizations Act (RICO) provides criminal penalties as well as a civil, private cause of action for acts performed as part of a criminal organisation or enterprise.[101] The statute contains variations on the proscribed conduct, but generally criminalises participation in an 'enterprise' in interstate or foreign commerce using ill-gotten gains that result from a 'pattern of racketeering activity'.[102] Such racketeering activity includes mail and wire fraud and money laundering violations under Sections 1956 and 1957, as outlined above.[103]

RICO violations are punishable by fines and imprisonment for up to 20 years, plus forfeiture of any interest acquired or maintained through the violation, any interest in any enterprise that was established, operated, controlled, conducted or participated in as part of the RICO violation (or the property of such an enterprise) and any property constituting or derived from any proceeds that the person obtained, directly or indirectly, from racketeering activity.[104]

Additionally, the government may seek pre-indictment restraining orders for the purpose of preventing defendants from transferring assets the government may potentially seek to have forfeited. To obtain such an order, the government must establish that (1) there is a substantial probability that it will prevail on the forfeiture issue, (2) property will be destroyed or placed beyond the court's reach without the order and (3) the need to maintain the property's availability outweighs the hardship of a restraining order. Pre-indictment restraining orders are effective for 90 days, but can be extended for good cause or as a result of the filing of an information or indictment.[105]

---

100 50 U.S.C. § 1705; 31 C.F.R. § 501; Congressional Research Service, 'The International Emergency Economic Powers Act: Origins, Evolution, and Use' (20 March 2019), available at https://fas.org/sgp/crs/natsec/R45618.pdf.

101 18 U.S.C. §§ 1961, et seq.

102 18 U.S.C. § 1962. The first variation makes it unlawful for any person who has received any income derived from a pattern of racketeering activity to use any part of such income or its proceeds to acquire, establish or operate any enterprise involved in interstate or foreign commerce. 18 U.S.C. § 1962(a). The second variation makes it unlawful for any person to engage in a pattern of racketeering activity to acquire or maintain any interest in any enterprise involved in interstate or foreign commerce. 18 U.S.C. § 1962(b). The third variation makes it unlawful for any person employed by or associated with any enterprise involved in interstate or foreign commerce to conduct the enterprise's affairs through a pattern of racketeering activity. 18 U.S.C. § 1962(c). The statute also makes it unlawful for a person to conspire to participate in the conduct outlined in (a), (b) or (c). 18 U.S.C. § 1962(d).

103 18 U.S.C. § 1961(1).

104 18 U.S.C. § 1963(a).

105 18 U.S.C. § 1963(d).

There are also civil remedies under RICO available to any person injured by a RICO defendant, which include treble damages sustained by the injured party and the cost of the lawsuit, including reasonable attorneys' fees.[106]

Conclusion 26.8

Corporates and individual may face a variety of fines, penalities and other collateral consequences when defending against or settling an enforcement action with US regulators. As has been explained, these risks can be substantial. That said, these risks can be managed, mitigated or avoided by engaging knowledgeable external counsel, who can evaluate the situation, provide advice and thereby enable the corporate or individual to make an informed decision about how to proceed.

106 18 U.S.C. § 1964(c).

27

Global Settlements: The In-house Perspective

Claire McLeod[1]

27.1 Introduction

Reaching a global settlement will involve engagement with multiple enforcement agencies across multiple jurisdictions and co-ordination of a significant number of external and internal stakeholders. Settlements are multifaceted and require consideration of many factors, including the commercial aspects, not just the penalty but also potentially redress or compensatory payments; the collateral consequences for the company; the impact on employees; continuing regulatory requirements; and potential follow-on litigation. The timing and sequencing of a global settlement with multiple agencies and regulators can also be key. One of the principle advantages for a corporate in reaching a global settlement is to achieve a resolution guaranteeing finality and certainty. If this cannot be achieved, or achieved with a high degree of certainty, a company has to consider whether the benefits of a more limited settlement outweigh a further period of uncertainty. This can be a complex and difficult decision, especially when some of the uncertainty may not be fully quantifiable. This chapter will look at these key considerations from the perspective of the different stakeholders in a global settlement.

27.2 Senior management

When considering global settlements, key considerations for senior management will be (1) the size of the financial penalty and any other financial components to the settlement; (2) the extent to which the settlement will bring finality of

1 Claire McLeod is the head of investigations and enforcement for Europe and the Middle East at Barclays Bank PLC. The views expressed are the author's own and do not represent the views of Barclays Bank PLC.

resolution to the company; (3) potential collateral consequences to the company's business; and (4) reputational damage.

In recent years the size of financial penalties levied against corporates has grown exponentially. Since the 2008 financial crisis, a 2017 study shows the 50 largest banks in the United States and Europe have paid over US$300 billion in penalties for regulatory breaches.[2] Negotiating the financial penalty of any global resolution will be a key consideration for senior management. For regulators and law enforcement agencies working within a fairly rigid penalty framework, the scope for negotiating the proposed penalty may be more limited. For others there may be greater scope to seek a more proportionate penalty by putting forward arguments about the calculation method or the applicability of different components, for example whether disgorgement is appropriate. Ultimately, senior management will need to understand and take into account the proportionality of the penalty and the impact it will have on the company's overall financial health.

In the United Kingdom, focused resolution agreements (FRAs) allow financial services firms to challenge a penalty proposed by the Financial Conduct Authority (FCA).[3] In April 2019, the FCA fined Standard Chartered Bank just under £102.2 million for anti-money laundering breaches.[4] This case was one of the first to involve a FRA. Standard Chartered agreed the FCA's findings of fact and liability, but argued that the proposed penalty was too high. Standard Chartered challenged the size of the penalty at a hearing before the FCA's Regulatory Decisions Committee (RDC), arguing that the proposed penalty was not proportionate based on the seriousness of the relevant breaches and certain mitigating factors. The RDC found in the bank's favour, reducing the penalty from £155 million to £102 million, which included maintaining a 30 per cent settlement discount – a term of the FRA.

In addition to financial penalties, there may be a further financial component of the resolution involving significant redress, compensatory payments or consumer relief. Indeed, a regulator may require this as part of any settlement.[5] The potential for financial impacts beyond the original penalties as a result of follow-on civil litigation must also be taken into account. Management will need to understand the total financial impact across all aspects of the settlement and any consequential financial impacts before deciding whether it is in the best interests of the company and its shareholders to proceed.

A key consideration for senior management will be the extent to which the settlement will bring finality of resolution for the company. The uncertainty created by a significant enforcement investigation, and what the outcome, business

2 See BCG Global Risk 2017: Staying the Course in Banking, http://image-src.bcg.com/BCG_COM/BCG-Staying-the-Course-in-Banking-Mar-2017_tcm9-146794.pdf.

3 The FCA introduced Focussed Resolution Agreements in March 2017.

4 https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls.

5 In 2017, the FCA used its powers under section 348 of the Financial Services and Markets Act to require Tesco plc and Tesco Stores Limited to pay compensation to investors for market abuse, https://www.fca.org.uk/news/press-releases/tesco-pay-redress-market-abuse.

impact and reputational damage will be, can often mean that settling with only one agency or on one aspect of the action is unlikely to be attractive. One of the main advantages to reaching a global settlement is being able to draw a line under the matter so that management can refocus their attention on their business and customers. However, this is not always easy to achieve. Co-ordinating a global settlement across multiple jurisdictions and agencies can be challenging, requiring the agencies synchronising the completion of their investigations and the corporate negotiating settlements simultaneously with each agency. Settling with one agency could also risk triggering an investigation by another with further (and in some cases heightened) risk to the company and additional uncertainty. In these circumstances, the company may consider it is not in its interests to seek an earlier settlement because the potential exposure and uncertainty remaining is too significant.

The likely collateral consequences of any resolution, in particular the potential impact on the company's business and customers will also be paramount. The risk of collateral consequences in recent years has become more acute as the number of corporate criminal actions has increased. These could include debarment from tendering for public procurement contracts, disqualification from – or restrictions on – specific business practices, and having to seek waivers from regulators to continue other business activities. These collateral consequences may dictate the terms on which a company is willing to enter a settlement. For example, deferred prosecution agreements (DPAs), rather than a guilty plea or conviction, could be beneficial to a company in avoiding certain collateral consequences. The DPA entered into by Rolls-Royce in 2017 allowed the company to avoid being debarred from tendering for public contracts.[6]

The potential (and often unquantifiable) reputational impact of a settlement should also not be underestimated. The company will want to plan a comprehensive strategy to minimise reputational damage. One aspect of this will be the proposed terms of the settlement, including the nature and extent of the factual and legal admissions required. Senior management will want to ensure that any admissions are supported by the evidentiary record and will want to understand if any of these admissions give rise to the risk of further regulatory or enforcement action or follow-on litigation. They will also want to take into account the reputational impact. These are key considerations for a company when negotiating the terms of any final statement of facts or agreement.

Other considerations will include any longer term impact on the company of any other settlement terms, for example the installing of a monitor or imposition of probationary terms. Monitors can be extremely costly, both in terms of financial costs and management time.

6 *Serious Fraud Office v. Rolls–Royce Plc* (Case No. U20170036) [2017] Lloyd's Rep FC 249, 'Debarment and exclusion would clearly have significant, and potentially business critical, effects on the financial position of Rolls-Royce. This could lead to the worst case scenario of a very negative share price impact, and, potentially, more serious impacts on shareholder confidence future strategy, and therefore viability.' *per* Leveson P at para. 55.

Taking all these commercial aspects into account, senior management will be looking for a settlement that achieves the highest degree of finality and the least impact on the business and its customers. The extent to which the company considers it has already addressed the root causes of the issues, and will be able to reassure its customers and employees that this is the case, will be critical.

Shareholders 27.3

A global settlement has to be in the interests of, and justifiable to, a company's shareholders. Many of the considerations cited above for senior management will also be key issues for the shareholders.

Aside from the level of the penalty and the impact it will have on the company's financial position, the single biggest concern for shareholders is likely to be achieving a final resolution. Shareholders will want to see the company move on and management be able to focus their attention on the business without the distraction of an ongoing enforcement action. A partial settlement or one that may trigger other litigation or enforcement action is unlikely to be considered a good outcome.

Shareholders will also expect the company to take appropriate action against any employees involved in the misconduct and will want to see that the company has taken steps to remediate any underlying issues. They will want assurance that the misconduct will not occur again, and they will want to have confidence that the current senior management of the company have set the right culture to ensure this. They will want to know that the company can properly move forward and draw a line under the matter.

Employees 27.4

An enforcement investigation and global resolution can have a significant and long-lasting impact on employees. In most enforcement matters involving a global organisation, the misconduct itself centres on a small part of the company, and a small number of employees. For those employees directly involved there will likely be a need to consider disciplinary proceedings and other issues such as the question of continuing to fund their legal representation and applicability of D&O insurance.

The majority of the company's employees, however, will know very little about the underlying issues until the settlement is announced. They will be most concerned about whether there will be any impact on them, including their ability to service their customers, and whether it will result in any changes to the structure or management of the company. Employees will also want to have confidence in senior management's handling of the matter, and the steps taken to remediate the underlying issues and prevent similar occurrences. It may also be important for employees to be able to communicate the measures taken to customers.

When a global settlement is announced, a company's management should provide sufficient information to employees to allow them to understand the rationale for the settlement, what it means in terms of reaching a final resolution, if there is going to be any impact on the company's business or customers, and, if

so, how this impact will be mitigated. It is also important for employees to know what they can communicate to customers, who may have many questions of their own about the potential impact of the settlement.

Despite not being involved in the underlying misconduct, the resultant negative reputational impact can still have an effect on employees, in terms of morale and motivation. It is therefore important for senior management to reassure employees that the matter has concluded, the company has taken appropriate action to address and remediate the issues, and to recognise the ongoing support and efforts of the wider employee workforce.

27.5 Customers

The single most important aspect of a global settlement for a company's customers is likely to be whether it will have any impact on the company's ability to continue servicing them. On announcement of a global settlement, customers will be looking for assurance, to the extent possible, that there will be no impact on the company's ability to continue doing business in the same way. To the extent there are restrictions or constraints placed on the company's business activities by the settlement, they will want to understand how the company will minimise the impact of these. Customers will also be looking for assurance that there will be continuity of service and the least disruption possible. This may involve structuring things differently or making changes to personnel. It will be important to identify all these issues and any contingencies planned well in advance of the settlement announcement.

Some customers may also want to know what changes the company has made to address the issues. This may be particularly important to customers or counterparties who conduct business on behalf of investors or shareholders to whom they owe fiduciary duties. This may also be more significant for customers where they consider there is a risk of an impact on their own compliance and regulatory obligations, for example if the misconduct involves anti-money laundering or sanctions breaches.

In recent years, some companies have considered that the risks of doing business in certain areas or jurisdictions are too high and have withdrawn from them. This 'de-risking' has been most prevalent in the banking industry and in respect of concerns about anti-money laundering (AML) and countering financing of terrorism (CFT), for example banks' withdrawal from business in areas such as the money transfer business sector. While this is unsurprising, there are broader socio-economic consequences, and concerns have been raised that this de-risking can in fact frustrate AML/CFT objectives by pushing higher risk transactions into more informal, unregulated channels that are harder to monitor.[7] More still needs to be done by governments, regulators and enforcement agencies to help banks mitigate the unintended consequences of de-risking.

7 De-risking in the Financial Sector, 7 October 2016, https://www.worldbank.org/en/topic/financialsector/brief/de-risking-in-the-financial-sector.

Regulators and enforcement agencies 27.6

The size of the monetary penalty is still considered one of the key aspects of a settlement by most regulators and enforcers. Credible deterrence is seen by many to require imposing a financial penalty so severe it affects the company's cost of doing business, to deter others at the company or in the industry from committing the same misconduct. Where multiple agencies are involved, there may also be political pressure to match equivalent penalties in other jurisdictions, increasing the overall settlement figure.

Another important aspect for the agencies in reaching a global settlement is often how the company will give redress to those who have been harmed by the misconduct.[8] If a company can demonstrate that it has voluntarily given redress for or remedied the misconduct in a timely and effective manner it is likely to receive credit for this in any final settlement.

The terms of any published statement of facts or final notice will also be important to make the severity and scale of the misconduct clear to the industry and wider public. The importance of this to the enforcement agency or regulator is often matched with the importance to the company of minimising the negative effects, which can make the negotiation of the terms hard-fought and the subject of contention.

In recent years, regulators and enforcement agencies have also placed a strong emphasis on holding individuals to account for the misconduct, both in terms of enforcement and disciplinary action. In 2018, the Department of Justice announced changes to its policy reflected in the Yates Memorandum[9] requiring companies to provide relevant information about 'all individuals substantially involved in or responsible for the misconduct'. It also reinforced its commitment to prosecuting the individuals responsible for the misconduct. In November 2018, Deputy Attorney General Rod J Rosenstein clarified that the Yates Memo's position on pursuing individuals remained a 'top priority', although he also announced a revised policy that gives prosecutors more discretion in deciding whether to pursue individuals.[10]

The introduction of the Senior Managers Regime by the FCA in the United Kingdom is also aimed at driving greater accountability within financial services firms. In 2015, the FCA and the UK Prudential Regulatory Authority (PRA)

8 See, for example, the FCA Mission: Our Approach to Enforcement, March 2018 (https://www.fca.org.uk/publication/corporate/our-approach-enforcement.pdf), in which the FCA places emphasis on the importance of taking action to address harm caused by serious misconduct.

9 Memorandum from Sally Quillian Yates, Deputy Attorney General, US Department of Justice to all US Attorneys, Individual Accountability for Corporate Wrongdoing (9 September 2015) https://www.justice.gov/archives/dag/file/769036/download.

10 Deputy Attorney General Rod J Rosenstein remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act, Office of Public Affairs, US Department of Justice, 29 November 2018, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

issued a joint policy statement[11] on the deferral of remuneration and clawback of variable compensation, and the FCA issued guidance setting out its expectations on how firms should comply with requirements on ex-post risk adjustment, to adjust variable remuneration to take into account a specific crystallised risk or adverse performance outcome including relating to misconduct.[12] In its guidance the FCA makes it clear that it expects firms to consider applying adjustments not just to those directly involved in the misconduct, but also to those employees whose roles and responsibilities include areas where failures or poor performance contributed to or failed to prevent the risk or misconduct.

Regulators and enforcement agencies will also want to see that the company has identified and remediated any root causes of the misconduct, including any systems and controls and cultural issues at the company. Credit is often given to those companies who take these steps proactively and at an early stage.

Finally, the extent to which a company is seen to have co-operated in the investigation is often a key determiner of the basis and terms of the settlement. In recent years, there has been much debate about the steps a company needs to take to be considered to have 'co-operated'. Some regulators and enforcement agencies have provided greater clarity and guidance in respect of what they consider constitutes co-operation.[13] However, there are differences in expectations across jurisdictions among agencies, making it important for companies to balance these expectations when co-ordinating a global investigation and settlement.

27.7 Conclusion

The increase and complexity of global settlements and the resultant collateral consequences in recent years means that early detection of a potential issue, through a robust compliance programme, has become all the more important. Effective and timely co-ordination of all aspects of the investigation, engagement with the different regulators involved, and consideration of the potential consequences and how to mitigate these, will be key factors in shaping the company's strategy for dealing with the matter. Identifying these issues and setting the strategy early on in the investigation is often key to ensuring that the sequencing and timing of a global settlement is ultimately achievable.

11 Strengthening the alignment of risk and reward: new remuneration rules, June 2015, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2015/ps1215.

12 Financial Conduct Authority, General guidance on the application of ex-post risk adjustment to variable compensation, 1 July 2015, https://www.fca.org.uk/publication/finalised-guidance/guidance-on-ex-post-risk-adjustment-variable-remuneration.pdf.

13 See, for example the Department of Justice's FCPA Corporate Enforcement Policy, https://www.justice.gov/criminal-fraud/file/838416/download and the SFO's Corporate Cooperation Guidance, https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook.

28

Extraterritoriality: The UK Perspective

Anupreet Amole[1]

Overview 28.1

English criminal law applies to all persons who come within the territory of England and Wales. In addition, there are now a number of mechanisms that enable UK authorities to investigate and prosecute offences committed overseas.

In the context of economic crime, the past three decades have seen a sustained legislative policy of extending the jurisdiction of the UK authorities. For certain economic crimes, authorities may bring prosecutions in the United Kingdom notwithstanding that all the relevant criminal conduct occurred overseas. The most obvious example is the Bribery Act 2010 (the Act), which we discuss further below. In line with the United Kingdom's extension of its jurisdictional reach, the authorities have increased their coordination and co-operation with other countries' prosecutors. The trend towards greater cross-border information sharing and coordinated investigations is likely to continue in accordance with ongoing domestic and international obligations.[2] The courts have also shown a willingness to endorse that trend. In the *KBR* case,[3] the High Court held that information

1 Anupreet Amole is a partner at Brown Rudnick LLP. The author thanks Aisling O'Sullivan and Charlotte Glaser and Francesca Cassidy-Taylor of the firm for their assistance with this chapter.

2 For example, the Common Reporting Standard (formally the Standard for Automatic Exchange of Financial Account Information) is an OECD initiative aimed at hindering tax evasion and money laundering. As of August 2019, there are over 100 signatories to the CRS (https://www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/). Similarly, the trend towards transparency is evident in recent statutory provision for implementing a register of beneficial owners of overseas corporate entities – see s.9 of the Criminal Finances Act 2017 and s.51 of the Sanctions and Anti-Money Laundering Act 2018.

3 *R (on the application of KBR, Inc) v. The Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin).

notices issued by the Serious Fraud Office (SFO) under section 2 of the Criminal Justice Act 1988 can have extraterritorial effect where a 'sufficient connection' exists between an overseas company and England and Wales. In particular, the court observed that SFO investigations should not be 'frustrated or stymied' on the basis that evidence may be held on computer systems located outside the jurisdiction. In April 2019, the Supreme Court granted KBR permission to challenge that decision, and the appeal is yet to be heard. This chapter provides an overview of the extraterritorial aspects of UK law regarding economic crime.

28.2 The Bribery Act 2010

In overview, the Act came into force on 1 July 2011 and created offences of (1) offering, promising or giving a bribe and (2) requesting, agreeing to receive or accepting a bribe either in the United Kingdom or abroad, in the public or private sectors, more specifically:

- sections 1 and 2 – bribing another person (active bribery) and being bribed (passive bribery);
- section 6 – bribery of a foreign public official; and
- section 7 – failure of commercial organisations to prevent bribery.

Each of the above offences has extraterritorial application, as outlined below.

28.2.1 Offences under sections 1, 2 and 6

UK prosecutors may pursue an offence under sections 1, 2 or 6, even where no act or omission forming part of that offence took place in the United Kingdom. This is the position provided that:

- a person's acts or omissions outside the United Kingdom would form part of such an offence if they had occurred in the United Kingdom;[4] and
- the person has a 'close connection with the United Kingdom'.[5]

A 'close connection with the United Kingdom' is defined in the Act and includes British citizens and UK companies.[6]

Considering a hypothetical example helps to demonstrate this broad jurisdictional scope of the Act. Assume that one Mr John Smith was born and raised in the United Kingdom, and, following university, he moved to live and work in Latin America. While Mr Smith has lived overseas for, say, 10 years, he has retained British citizenship. Mr Smith is a business consultant in the oil and gas

4 s.12(2)(b).

5 s.12(2)(c).

6 s.12(4). A person has a close connection with the United Kingdom if, and only if, the person was one of the following at the time the acts or omissions concerned were done or made: a body incorporated under the law of any part of the United Kingdom, a British overseas territories citizen, a British national overseas, a British overseas citizen, a person who under the British Nationality Act 1981 is a British subject, a British protected person under the British Nationality Act 1981, an individual ordinarily resident in the United Kingdom, or a Scottish partnership.

sector, and one of his key clients is an energy company based in India. Assume also that Mr Smith bribed a person in, say, Mexico, and did so in the course of his services to the Indian company, and in so doing he intended that he would obtain or retain business (in Mexico) for the Indian company. Even where none of Mr Smith's conduct made any contact with the United Kingdom, he would be at risk of criminal prosecution in the United Kingdom because he was a British citizen at the time of the offence, and therefore had a 'close connection' to the United Kingdom as defined by section 12(3) of the Act. In practice, of course, a prosecutor would need to consider carefully whether proceedings against Mr Smith would ultimately be in the public interest both in itself and as part of a wider prosecution strategy against others; in this case, for example, the Indian company if it had been carrying on business in the United Kingdom.[7]

Corporate offence under section 7 28.2.2

This offence is committed by a 'relevant commercial organisation' if a person associated with the organisation (an associated person)[8] bribes another person intending to obtain or retain business, or an advantage in the conduct of business, for the organisation. In those circumstances, the organisation's only defence to the strict liability offence is to show that it had 'adequate procedures' in place designed to prevent bribery on its behalf.[9]

A 'relevant commercial organisation' includes a company or partnership (wherever incorporated) that carries on any part of its business in the United Kingdom. On the basis of information in the public domain currently, the courts are yet to consider a case where it is disputed that a commercial organisation indicted under section 7 was carrying on business within the United Kingdom.[10] Until the courts hear argument on that specific point, practitioners continue to refer to the Ministry of Justice guidance regarding the corporate offence. That guidance recommends a 'common sense approach' and notes that a 'demonstrable business presence' is required. Neither having the company's shares listed on

7 Note that pursuant to s.14 of the Act, if a section 1, 2 or 6 offence was committed with the 'consent or connivance' of a 'senior officer' of a body corporate, or a person purporting to act in such a capacity, the senior officer (and the body corporate) is guilty of an offence.

8 An 'associated person' is defined in the Act as a person who performs services for or on behalf of the company in any capacity (i.e., an employee, agent or subsidiary), which is to be determined by reference to all the relevant circumstances and not merely the nature of his or her relationship with the company. It is worth bearing in mind that a section 7 offence will be committed only if the associated person intended to obtain or retain business or an advantage in the conduct of business for the relevant organisation.

9 s.7 of the Act. Although 'adequate procedures' is not defined in the Act, the Ministry of Justice's guidance (March 2011) broadly outlines what businesses need to demonstrate to mount a successful 'adequate procedures' defence, for example proper risk-assessment procedures, due-diligence protocols and top-level commitment.

10 The section 7 offence is in addition to, and does not displace, liability that might arise under the Act where the commercial organisation itself commits an offence by virtue of the common law 'identification' principle. For more information on the common law 'identification principle' see the Introduction of this book.

the London Stock Exchange nor having a UK subsidiary would necessarily mean that a foreign company is carrying on business for the purposes of section 7 of the Act.[11]

For a high-profile application of the concept of an associated person, the case of *Sweett Group PLC*[12] (2015), the SFO's first corporate conviction under section 7, is instructive. The defendant, a UK company, pleaded guilty to failing to take reasonable steps to prevent the bribery of a non-UK national in the United Arab Emirates by a Sweett Group subsidiary in Cyprus (Cyril Sweet International Limited); the bribe being paid to secure a contract relating to construction of a £63 million hotel in Dubai. Sweett agreed with the SFO's contention, via plea, that its subsidiary was an 'associated person' under the Act, and the court was satisfied that the bribes were intended to obtain an advantage in the conduct of business for Sweett. A financial penalty, taking into account the guilty plea, of £2.25 million was levied against Sweett.[13]

It is irrelevant whether the acts or omissions forming part of the section 7 offence took place in the United Kingdom or elsewhere.[14] Therefore, it is possible for either of the following scenarios to form the factual basis for a section 7 offence:

- any business formed or incorporated in the United Kingdom, where the bribery is conducted entirely outside the United Kingdom by an associated person who has no connection with the United Kingdom and who is performing services outside the United Kingdom; and
- any business formed or incorporated outside the United Kingdom, but that carries on part of its business in the United Kingdom, where the bribery is conducted entirely outside the United Kingdom by an associated person who has no connection with the United Kingdom and who is performing services outside the United Kingdom.

In August 2019, the SFO published its long-awaited Corporate Co-operation Guidance (the Guidance),[15] aimed at providing organisations and their legal advisers with transparency about what to expect if they self-report bribery to the SFO.

The Guidance sets out a non-exhaustive list of good practices for co-operation, including providing 'relevant material that is held abroad, where it is in the possession or under the control of the organisation'.[16] This codifies the approach

11 Ministry of Justice Guidance to the Bribery Act 2010 (March 2011), paras. 34-36.

12 See https://www.sfo.gov.uk/cases/sweett-group/.

13 This figure comprised a £1.4 million fine, a confiscation order of £850,000 and an order for costs to the SFO of £95,000.

14 s.12(5) Bribery Act 2010.

15 SFO Operational Handbook, Corporate Co-operation Guidance (https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/), accessed 14 November 2019.

16 Ibid. Preserving and providing material, para. 1(ix).

adopted in *KBR*,[17] whereby the SFO was able to compel a foreign company to produce documents outside the jurisdiction.

Bringing material located abroad into the jurisdiction of England and Wales may lead to legal arguments relating to its collateral use in subsequent civil or regulatory proceedings, as in *Omers Administration Corporation and others v Tesco Plc*.[18] While that case related to documents held in England and Wales, the High Court ordered that documents provided to Tesco by the SFO during negotiations for a deferred prosecution agreement should be disclosed by Tesco in a separate and subsequent civil action, brought by its shareholders. Companies and their advisers should note the implications of this in relation to bringing documents into the jurisdiction or providing documents, at least voluntarily, to the SFO, or other authority, in circumstances where that information may then be disclosed (1) by the SFO to the subjects of its relevant investigations, and (2) subsequently, to third parties through any relevant, separate civil proceedings brought against the subjects under SFO scrutiny.

Money laundering offences under Part 7 of POCA 2002 28.3

Money laundering has a broad meaning under UK law. The money laundering regime is designed to tackle the routes through which the proceeds of criminal activity are handled. The principal offences are found in sections 327 to 329 of the Proceeds of Crime Act 2002 (POCA), being:

- concealing, disguising, converting, transferring or removing from the United Kingdom, any criminal property (section 327);
- entering or becoming concerned in arrangements that one knows or suspects facilitate the acquisition, use, etc., of criminal property (section 328); and
- acquiring, using or possessing criminal property (section 329).

Property is 'criminal property' if it represents a person's benefit from criminal conduct; in turn, 'criminal conduct' is conduct that either is an offence in the United Kingdom or would be an offence if it had taken place within the United Kingdom.[19] Although the prosecution must adduce evidence of a predicate offence from which the proceeds of crime emanate, a prosecutor need not prove the type of predicate offence in every instance. Instead, the prosecutor will need to provide the court with detailed particulars explaining why the property that is the subject of the money laundering offence should be regarded as criminal in origin, and that evidence should be sufficiently potent to demonstrate that the only reasonable inference is that the property arose from criminality.

In the case of *R v. Anwoir*,[20] the appellants had been convicted of a number of money laundering offences under section 328 of POCA. They appealed on the

17 *R (on the application of KBR, Inc) v. The Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin).

18 *Omers Administration Corporation and others v. Tesco Plc* [2019] EWHC 109 (Ch).

19 s.340(2) and (3) POCA 2002.

20 *R v. Anwoir* [2008] EWCA Crim 1354.

basis that the prosecution should have been required to prove at least the class or type of criminal conduct involved in generating the criminal property. Allowing the appeal in part, the court held that there were two ways it could be proved that property had derived from crime. One was by showing that it derived from conduct of a specific and unlawful nature. The second method was by evidence of the circumstances in which the property was handled that gave rise to the irresistible inference that it could only have been derived from crime.[21]

The location of the underlying criminal conduct is immaterial. Instead, the pertinent issue is whether the conduct would constitute a criminal offence in the United Kingdom had it occurred here. This principle was confirmed by the Court of Appeal in 2014 in the case of *R v. Rogers*,[22] which served to emphasise the wide scope of the money laundering regime. Mr Rogers, a UK citizen resident in Spain, permitted money generated by a fraudulent scheme in the United Kingdom to be paid into a Spanish bank account that he controlled, and allowed another person, the scheme's principal, to withdraw money from that account. Mr Rogers was convicted under section 327(1)(c) of POCA of converting criminal property. He subsequently appealed against that conviction, arguing that the court did not have jurisdiction to hear Part 7 offences against a non-UK resident where the relevant conduct occurred entirely outside the United Kingdom.

In dismissing the appeal, the court expressly considered the wording of section 340(11)(d) of POCA, that money laundering is an act that would constitute an offence under sections 327, 328 or 329 if done in the United Kingdom, and concluded that the language clearly indicated that Parliament had intended for the Part 7 offences to be extraterritorial in effect. (It is arguable that this amounts to a misreading of the statutory provisions because section 340(11) defines 'money laundering' for the purposes of the reporting obligations set out in sections 330 to 332 and, for that obligation, it does not matter whether the money laundering takes place in the United Kingdom or abroad. In contrast, the term 'money laundering' does not appear as a constituent element of the offences in sections 327 to 329 of POCA.) The court went on to state that, even if they were wrong on that interpretation of the statute, the modern approach to jurisdiction required 'an adjustment to the circumstances of international criminality', and noted: 'The offence of money laundering is *par excellence* an offence that is no respecter of national boundaries. It would be surprising indeed if Parliament had not intended the Act to have extra-territorial effect (as we have found it did).'[23]

In light of this extraterritorial effect, the court was able to establish a sufficient jurisdictional nexus to try Mr Rogers on the basis that the acts that led to the property becoming criminal property for the purposes of POCA plainly took

21 This case has since been applied by the Court of Appeal in *R. v. Anwar (Nasar)* [2013] EWCA Crim 1865.

22 [2014] EWCA Crim 1680. This case was applied in *Jedinak v. Czech Republic* [2016] EWHC 3525 (Admin) and followed in *Sulaiman v. France* [2016] EWHC 2868 (Admin).

23 *R v. Rogers* (Bradley) *and others* [2014] EWCA Crim 1680 (*per* Treacy LJ) at p. 1026, paras. 52 and 54.

place, and had an impact on victims, in the United Kingdom, and that the laundering of the proceeds by Mr Rogers in Spain was directly linked to those acts in the United Kingdom. The court added that this was:

> *not a case where the conversion of criminal property relates to the mechanics of a fraud which took place in Spain and which impacted upon Spanish victims. In those circumstances our courts would not claim jurisdiction. But in this case when the significant part of the criminality underlying the case took place in England, including the continued deprivation of the victims of their monies, there is no reasonable basis for withholding jurisdiction . . . .*[24]

The court's decision in *Rogers* makes plain that UK persons based overseas, including, for example, professional legal or tax advisers, face the risk of criminal liability in the United Kingdom for money laundering offences committed wholly overseas. *Rogers* and subsequent cases indicate that a person may be guilty of a money laundering offence under sections 327 to 329 of POCA in circumstances where both the predicate offending (ie, the criminality that gives rise to the existence of proceeds of crime) and the laundering of the criminal property take place outside the territory of the United Kingdom.[25]

There exists a limited exception described as the 'overseas conduct defence'. A person will not be liable under sections 327 to 329 if:

- he or she knew or reasonably believed that the relevant criminal conduct occurred abroad; and
- that relevant criminal conduct was not, when it took place, unlawful under the criminal law of that other country.[26]

The 'overseas conduct defence', however, does not apply to conduct that (despite being legal under local law) would constitute an offence punishable by a maximum sentence of imprisonment over 12 months in the United Kingdom if it had occurred in the United Kingdom.[27] In practice, therefore, most cases (e.g., bribery,

24 Ibid. (*per* Treacy LJ) at pp. 1026–1027 at para. 55.

25 *Sulaiman v. Tribunal de Grande Instance* [2016] EWHC 2868 (Admin) in which Dingemans J confirmed that *Rogers* is 'binding' authority 'for the proposition that offences of money laundering extend to extraterritorial actions' (at [18]) and *Jedinak v. District Court in Pardubice* [2016] EWHC 3525. The implication of these decisions is that, while *Rogers* suggests that cases where both the predicate offence and the money laundering offence take place overseas might be decided differently, in fact in cases decided subsequent to *Rogers* this has not been the case. In *Jedinak* despite the arguments by the defence that 'the court was clearly to an extent motivated by the recognition that some part of the offending [in *Rogers*] (and indeed the damage cause by the offending) impacted on this country and nationals of this country', the court held that 'it is clear in my judgment that the decision relating to the possible extra-territorial effect of the money laundering offences was independent of that'.

26 ss.327(2A), 328(3) and 329(2A) POCA 2002.

27 The Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order 2006.

corporate fraud, tax evasion) relevant to readers will remain squarely within the wide extraterritorial scope of POCA.

28.3.1 The Fourth Money Laundering Directive (4MLD)

The POCA 2002 regime has been further supplemented by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, which gave effect to the European Union's Fourth Money Laundering Directive.[28] The 2017 regulations apply to both financial institutions and to over 100,000 businesses that may be considered the 'gatekeepers' of the financial system.[29] Those 'gatekeepers' include, for example, legal advisers, insolvency practitioners, casinos and dealers in high-value goods. The 2017 regulations provide for a 'risk-based' approach to money laundering and provide *inter alia* for reforms to risk assessments, customer due diligence and employee screening. The 2017 regulations also provide for a number of criminal offences, which are given extraterritorial effect through Regulation 90, which enables courts to treat offences 'committed wholly or partly outside the United Kingdom' as 'having been committed within the jurisdiction of the court'.

The scope of the 2017 regulations has been extended to cover the operations of subsidiaries and branches operated by a 'relevant person'[30] outside the United Kingdom.[31] Where the relevant person is operating in a European Economic Area state that has implemented the 4MLD, it must follow the law of that state. Significantly, if the subsidiary or branch is operating in a country that has not implemented the 4MLD, it must comply with the regime as implemented in England and Wales.

28.3.2 Civil recovery orders

Separately, the civil recovery regime set out in POCA[32] enables UK prosecutors to seek orders from the High Court to recover property that either is or represents property obtained through unlawful conduct. As applications for civil recovery orders and property freezing orders are determined through civil, not criminal, proceedings before the High Court, the standard of proof is the balance of probabilities. The High Court may issue such an order against any person or property wherever domiciled or situated, if there is or has been a connection between the

28 The regulations came into force on 26 June 2017, giving effect to Directive 2015/849. The previous regime, governed by the Money Laundering Regulations 2007 and the Transfer of Funds (Information on the Payer) Regulations 2007 was revoked.

29 Explanatory Memorandum to the regulations, p. 2.

30 Namely a person to whom the regulations apply, as defined by Regulation 8, Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

31 Regulation 20, Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

32 Part 5 of POCA 2002.

facts of the case and any part of the United Kingdom.[33] Combined with the wide jurisdictional scope of the definition of 'unlawful conduct',[34] civil recovery orders are a powerful and attractive tool in the hands of UK prosecutors. While foreign courts did not traditionally recognise the enforceability of these orders against assets in their jurisdictions, a relatively recent case saw the United Kingdom's National Crime Agency (NCA) succeed in persuading the Luxembourg court to enforce an order against a UK person's bank accounts in that jurisdiction.[35] This was the first time that a foreign court had enforced a civil recovery order, permitting the NCA to recover unlawful property held entirely outside the United Kingdom. It remains to be seen whether other jurisdictions will take a similarly collaborative approach to UK civil recovery efforts overseas.

See Chapter 25 on fines, digorgement, etc.

An additional civil recovery power became available to the NCA and other UK prosecutors in late January 2018.[36] On application to the High Court, prosecutors can seek an unexplained wealth order (UWO) against any persons (whether or not UK domiciled) regarding their property, irrespective of that property's location. In summary, a UWO is available where:

- there is reasonable cause to believe the respondent holds specific property valued at or above £50,000;
- there are reasonable grounds to suspect that the respondent's known income is insufficient to acquire that property; and
- either the respondent is a 'politically exposed person' or there is reasonable suspicion that the respondent (or a person connected to him or her) is or has been involved in serious crime in the United Kingdom or abroad.

Where granted, the UWO compels the respondent to explain the nature of their interest in the property, and to explain how they obtained it. Failure to do so creates a presumption that the property was obtained unlawfully, and it is therefore a valid target for civil recovery proceedings under Part 5 of POCA.

The respondent, namely the person who holds or obtains the relevant property, 'includes any body corporate, whether incorporated or formed under the law of a part of the United Kingdom or in a country or territory outside the United

33 s.282A POCA 2002, inserted by s.48 of the Crime and Courts Act 2013 following the UK Supreme Court decision in *Perry v. SOCA* [2012] UKSC 35. s.282A and Schedule 7A POCA have retrospective effect – see para. 7(7) of Schedule 7A POCA.

34 Defined as (1) conduct within the United Kingdom that is unlawful under UK criminal law or (2) conduct outside the United Kingdom that is unlawful in that other country and would have been unlawful in the United Kingdom, had it occurred here. This is, therefore, a dual criminality test. The recent insertion of a new s.241A POCA 2002 (by s.13 of the Criminal Finances Act 2017) adds 'gross human rights abuse or violation' to the definition of unlawful conduct for the purposes of Part 5 POCA (civil recovery). This is the United Kingdom's introduction of the concept of targeting assets owned by those involved in repressive regimes anywhere in the world; this follows the approach in the United States to a statute known as the Magnitsky Act of 2012.

35 *National Crime Agency v. Azam* [May 2015], District Court of Luxembourg.

36 See Part 1 of the Criminal Finances Act 2017, which amends POCA.

Kingdom.'[37] By express cross-reference to section 414 of POCA,[38] it is clear that 'property is all property wherever situated'.

Where a UWO is granted against property outside the United Kingdom, and the UK prosecutor believes there is a risk of dissipation or frustration by concealing the relevant assets, that prosecutor may make a formal request for assistance from the other country's government.[39] The use of UWOs remains a developing area of practice, and one to watch closely in light of the authorities' recent success in the case of *National Crime Agency v. Mrs A.*[40] As of July 2019, the National Crime Agency had obtained four UWOs, the most recent cases being against (1) a person in Northern Ireland with suspected links to paramilitary and organised crime activities, and (2) an individual in northern England suspected of using funds from associates involved in drug and firearms trafficking to finance his acquisition of real property.

See Chapter 30 on individual penalties, etc.

28.4 Tax evasion and the Criminal Finances Act 2017

The Criminal Finances Act 2017 also introduced a new corporate offence focused on tax evasion. As with the Bribery Act's corporate offence, this represents another significant departure from the traditional 'directing mind' identification doctrine for corporate criminal liability under English law.

See Chapter 1

Part 3 of the Criminal Finances Act 2017 creates two new corporate offences of failure to prevent the facilitation of tax evasion. The offences are modelled on section 7 of the Bribery Act 2010 and apply to both domestic and overseas tax evasion. The new offences are:

See Section 28.2.2

- failure to prevent the facilitation of UK tax evasion offences (section 45): a company or partnership is guilty of an offence if a person commits a UK tax evasion facilitation offence when acting in the capacity of a person associated with that company or partnership;[41] and
- failure to prevent the facilitation of foreign tax evasion offences (section 46): a company or partnership is guilty of an offence if at any time a person commits a foreign tax evasion facilitation offence when acting in the capacity of a person associated with that company or partnership, and any of the following conditions is satisfied:
  - the relevant body is incorporated or formed in the United Kingdom;
  - the relevant body carries on business or part of a business in the United Kingdom; or
  - any conduct constituting part of the foreign tax evasion facilitation offence took place in the United Kingdom.[42]

37 s.362H(5) POCA, inserted by s.1 CFA 2017.

38 s.362H(6) POCA, inserted by s.1 CFA 2017.

39 s.362S POCA, inserted by s.3 CFA 2017.

40 [2018] EWHC 2534 (Admin).

41 The UK tax offence will be investigated by Her Majesty's Revenue and Customs (HMRC), with prosecutions brought by the Crown Prosecution Service.

42 s.46(2).

If the offence took place outside the jurisdiction, however, UK prosecutors must still prove to the criminal standard that both the taxpayer and the associated person committed an offence. The prosecutor will also need to prove dual criminality of the conduct. The offences consist of three component parts. First, the prosecution must prove criminal evasion by a taxpayer; and there must have been dishonest[43] facilitation of tax evasion by an associated person. Where these two components are satisfied, the relevant body is criminally liable (unless it can show that it had 'reasonable preventative procedures' in place, or that it was unreasonable to expect the company to have had such procedures in place).

A 'relevant body' is a company or a partnership, wherever it may be incorporated or formed.[44] A 'person associated' with the relevant body is an employee, an agent or any other person performing services for or on behalf of that relevant body.[45] Again, this is broadly comparable to the concepts in the Bribery Act. Section 46 of the Criminal Finances Act 2017 provides that a company or partnership that carries on business in the United Kingdom will commit an offence if a 'person associated' with it commits a 'foreign tax evasion facilitation offence', unless the company or partnership had reasonable procedures in place to prevent the facilitation offence. A foreign tax evasion facilitation offence means conduct that amounts to:

> *an offence under the law of a foreign country . . . relates to the commission by another person of a foreign tax evasion offence under the law of that country, and . . . would, if the foreign tax evasion offence were a UK tax evasion offence, amount to a UK tax evasion facilitation offence . . . .*[46]

The UK government recently published guidance on the meaning of reasonable preventative procedures.[47] The guidance states that those procedures should be informed by the same six guiding principles as those expected by the Bribery Act model. The six principles are proportionality, top level/board level commitment, risk assessment, due diligence, training and communication, and monitoring/review. Companies doing business in the United Kingdom should consider carefully how to prepare their own reasonable preventative procedures to address the risk of associated persons facilitating tax evasion.

---

43 The test for dishonesty must now be viewed in light of the Supreme Court's decision in *Ivey v. Genting Casinos (UK) Ltd t/a Crockfords* [2017] UKSC 67 which disapproved the second limb of the well-known test in *R v. Ghosh* [1982] EWCA Crim 2. Although the observations of the court were technically *obiter*, the Court of Appeal (Criminal Division) has indicated that *Ivey* correctly reflects the law – see *R v. Pabon* [2018] EWCA (Crim) 420.

44 s.44(2) and (3)

45 s.44(4).

46 s.44(6).

47 Tackling tax evasion: Government guidance for the corporate offences of failure to prevent the criminal facilitation of tax evasion, HM Revenue and Customs, 1 September 2017, available at https://www.gov.uk/government/publications/corporate-offences-for-failing-to-prevent-criminal-facilitation-of-tax-evasion.

28.5 Financial sanctions

While they are driven by geopolitical issues, international sanctions have direct practical and legal consequences for businesses of all shapes and sizes. The use of international sanctions has grown over recent years, particularly in relation to the military conflicts in Ukraine and Syria. In fact, this continues a trend that began in modern times with the United Nations' Oil-For-Food Programme regarding Iraq after the Gulf War of 1991. At the time of writing, the United Kingdom applies financial sanctions in 27 separate programmes, targeting governments and terrorist groups such as the governments of Burundi, North Korea and Syria, and the Taliban, ISIL and Al-Qaida.

Financial sanctions restrict the provision of financial services, or access to global capital markets, or both. More specifically, those restrictions can include bans on investments in a particular country, or the denial of banking relationships. Trade sanctions restrict the trading of certain products or commodities (e.g., arms, oil and diamonds) from targeted countries (e.g., Iran, Russia and Syria) and control the export of certain products (e.g., military or dual-use items) to targeted countries. A recent decision by the European Court of Justice, which upheld the EU sanctions against Russia regarding its annexation of Crimea in 2014, demonstrates the rationale in practice:

> *Contrary to what is claimed by Rosneft, there is a reasonable relationship between the content of the contested acts and the objective pursued by them. In so far as that objective is, inter alia, to increase the costs to be borne by the Russian Federation for its actions to undermine Ukraine's territorial integrity, sovereignty and independence, the approach of targeting a major player in the oil sector, which is moreover predominantly owned by the Russian State, is consistent with that objective and cannot, in any event, be considered to be manifestly inappropriate with respect to the objective pursued.*[48]

For the purposes of this chapter, we focus on financial sanctions.[49] The UK legal framework regarding financial sanctions is not contained in any one particular statute. Instead, the United Kingdom uses secondary legislation to implement various sanctions programmes made by each of the United Nations Security

48 *PJSC Rosneft Oil Company v. Her Majesty's Treasury and Others*, Case C-72/15, 28 March 2017 at 147.

49 For trade sanctions, see the Export Control Act 2002 (and the related Export Control Order 2008) and the Customs and Excise Management Act 1979. The Customs and Excise Management Act 1979 imposes criminal liability where a person exports goods from the United Kingdom 'when the exportation or shipment is or would be contrary to any prohibition or restriction for the time being in force'. The Export Control Order 2008 imposes those restrictions. The ECO 2008 specifies a three-tier categorisation of goods, with Category A products including items designed for torture; Category B includes arms and ammunition; Category C being items that have a dual civil/military use. See Part 4 and Schedule 1 of the ECO 2008. Trade sanctions apply to (1) anybody present in the UK, i.e., all persons (natural and legal); (2) all UK subjects anywhere in the world; and (3) any legal entity incorporated under UK law.

Council and the European Union. At the same time, the United Kingdom may also issue domestic financial sanctions under certain specific statutes, such as the Terrorist Asset-Freezing Act 2010.[50] The specific restrictions imposed by any one set of financial sanctions (e.g., those relating to Russia's involvement in Ukraine) will vary in each case. Those advising businesses concerned about liability should carefully review the text of the specific statutory instrument, and the underlying EU regulation, in each case. Broadly, however, UK financial sanctions impose criminal liability for a person who:

- makes funds or economic resources available, whether directly or indirectly, to a designated person;
- deals with funds or economic resources belonging to or controlled by a designated person; or
- acts in a way, whether directly or indirectly, to circumvent the relevant financial sanction prohibitions.[51]

Financial sanctions also carry positive reporting obligations for financial services firms. Where a firm detects relevant information, for example that a customer or counterparty is a designated person, the firm must notify the Office of Financial Sanctions Implementation (OFSI), which is part of HM Treasury.[52]

While the jurisdictional scope of UK financial sanctions is broad, they do require some element of UK nexus. The sanctions apply to:

- anybody present in the United Kingdom, namely all persons (natural and legal) 'who are within or undertake activities within the UK's territory'; and
- all UK nationals and all UK legal entities (including branches, and the UK subsidiaries of foreign companies), wherever they may be in the world and irrespective of where their activities occur.[53]

In recent guidance, the OFSI emphasised that establishing a UK nexus would be determined by the facts in each case, and that it would not seek to 'artificially bring something within UK authority that does not clearly and naturally come under it'.[54] This may provide some degree of comfort to foreign businesses with no UK footprint. Most recently, the new Sanctions and Anti-Money Laundering Act 2018, which is not yet fully in force, provides for sanctions being imposed regarding (1) conduct within UK jurisdiction by any person and (2) conduct anywhere in the world but only if the conduct is by a 'United Kingdom person'.[55]

---

50 The other relevant UK statutes, which also take a broad jurisdictional approach, are the Counter-Terrorism Act 2008 and the Anti-terrorism, Crime and Security Act 2001.

51 Office of Financial Sanctions Implementation, Financial Sanctions: Guidance, March 2018, p. 12. The maximum term of imprisonment was recently increased from two to seven years – see ss.144 and 145 of the Policing and Crime Act 2017 (PCA 2017).

52 Office of Financial Sanctions Implementation, Financial Sanctions: Guidance, March 2018, p. 18.

53 Office of Financial Sanctions Implementation, Financial Sanctions: Guidance, March 2018, p. 7.

54 Office of Financial Sanctions Implementation, Monetary penalties for breaches of financial sanctions: Guidance, May 2018, p. 12.

55 s.21 Sanctions and Anti-Money Laundering Act 2018.

Until recently, enforcement options were limited, taking the form of either an official warning letter from HM Treasury or full criminal proceedings by a prosecutor. The Policing and Crime Act 2017, effective from 3 April 2017, introduced a wider range of enforcement options, specifically (1) making sanctions offences eligible for consideration for a deferred prosecution agreement,[56] (2) making sanctions offences eligible for (civil) Serious Crime Prevention Orders under the Serious Crime Act 2007[57] and (3) empowering the OFSI to impose (civil) financial penalties.[58] These developments are all consistent with the general trend in UK law since the Bribery Act 2010 came into effect towards increased enforcement against companies, including for misconduct overseas.

28.6 Information sharing powers under the Criminal Finances Act

As demonstrated by several recent enforcement actions, the UK authorities have increased their sharing of information with counterparts around the world. That coordination is developing further. The Criminal Finances Act 2017 includes certain amendments to POCA, the effect of which will be to enhance the information flow to the UK authorities (specifically, the NCA in the first instance),[59] and most importantly for the purpose of this chapter, to facilitate the NCA's assistance of law enforcement bodies overseas.

28.7 Conspiracy

Readers will be familiar with cases involving suspected or alleged conspiracies to commit substantive offences. When considering conspiracy in the economic crime context, practitioners should be aware of the interplay between (1) common law conspiracy to defraud, (2) the conspiracy offence in section 1A Criminal Law Act 1977, and (3) the Fraud Act 2006, whose extraterritorial reach is specified by the Criminal Justice Act 1993 (as amended).

56 s.150 of PCA 2017.

57 s.151 of PCA 2017.

58 s.146 of PCA 2017.

59 Section 10 of the Act serves to extend the moratorium period for investigations into suspicious activity reports (SARs) and provides the NCA with new powers to request information from regulated companies. Under this section, a 'senior officer' of a relevant authority can apply to the Crown Court for an extension of the current seven-working-day moratorium period for SARs. If the application is granted, the court can extend the moratorium period for no more than a further 186 days. The court will only be in a position to grant an extension of 31 days at a time, with the relevant authority being required to continue to make further applications for additional extensions should it be deemed necessary. This will enable the court to exercise judicial scrutiny over the relevant authorities. If an application is refused by the court, the relevant authority has a further 31 calendar days in which it can investigate and either take action to freeze the funds or give its consent to proceed with the transaction.

Common law conspiracy to defraud 28.7.1

The leading case defines a conspiracy to defraud as an agreement 'to deprive a person dishonestly of something which is his or to which he is or would be or might be entitled' or 'by dishonesty to injure some proprietary right'.[60]

Common law conspiracy to defraud is one of the very few remaining common law conspiracy offences, section 5 of the Criminal Law Act 1977 having replaced all others with a general statutory offence. The rationale for its retention despite the statutory offences introduced by the Fraud Act 2006 was that the common law offence was broad (as indicated by the definition above), and therefore allowed prosecutors to roll several offences into a smaller number of indictments than would otherwise be required to prosecute multiple examples of fraudulent conduct, and present a single cogent narrative to the court, without needing to charge, and evidence, several separate statutory offences.[61] Statute has made clear that a person charged with conspiracy to defraud may be liable irrespective of whether he or she became a co-conspirator in England or whether any act in relation to the conspiracy occurred in England.[62]

Statutory conspiracy to commit offences abroad 28.7.2

The Criminal Justice Act 1987 provides that a prosecutor may pursue common law conspiracy to defraud even in circumstances where the substantive offence would be covered by a specific statute.[63] However, in many cases, ranging from *Innospec Limited*[64] in 2010 to the recent attempted prosecution of Barclays Bank regarding Qatar, the SFO has relied on section 1(1) of the Criminal Law Act 1977 to bring charges of conspiracy to commit offences.[65]

In 1998, the Criminal Law Act 1977 was amended to provide expressly for a discrete offence of conspiracy to commit criminal offences outside the

60 *Scott v. Metropolitan Police Commissioner* [1975] AC 819 at 840F.

61 See the Attorney General's Guidance on use of the common law offence of conspiracy to defraud, (2007), and the Ministry of Justice Post-Legislative assessment of the Fraud Act 2006 (June 2012).

62 s.3(2) Criminal Justice Act 1993.

63 s.12 Criminal Justice 1987, which retained the offence at common law of conspiracy to defraud – see s.5(2) Criminal Law Act 1977.

64 The charge against Innospec Ltd was that between February 2002 and December 2006, the company, through various agents, engaged in systematic and large-scale corruption of senior government officials of Indonesia to secure contracts for the supply of a fuel additive, tetraethyl lead (TEL). The corrupt behaviour took the form of bribes, totalling approximately US$8 million. The seriousness of the corruption was aggravated by the fact that Innospec Ltd's behaviour was aimed at blocking legislative moves to ban TEL, owing to environmental and public health concerns. The company pleaded guilty to conspiracy contrary to s.1 of the Criminal Law Act 1977 and was fined US$12.7 million.

65 In *R v. Turner*, *Kerrison, Papachristos and Jennings* in 2014 (and the subsequent appeal *SFO v. Papachristos and Kerrison* [2014] EWCA Crim 1863), four former executives of Innospec were convicted and imprisoned for conspiracy offences in relation to their roles in bribing state officials in Indonesia and Iraq in order to secure contracts from the governments of those countries for the supply of products produced by Innospec Ltd.

jurisdiction.[66] By section 1A of the Act, a conspiracy may involve the doing of an act in a place outside England and Wales that constitutes an offence in that other jurisdiction. The purpose of section 1A was to extend existing UK law, and to give the English courts extraterritorial jurisdiction in relation to a conspiracy (1) partly formed or carried out in England and Wales, and (2) where the object was the commission of a foreign offence (where there is an equivalent offence in England and Wales). This section only applies, however, where four nexus conditions are satisfied:

- pursuit of the agreed conduct would involve an act by one or more of the parties outside the United Kingdom;
- that act is an offence under local law in that other country;
- that the agreement would be a conspiracy (within section 1(1) CLA 1977) but for the fact that the offence would not be an offence triable in England and Wales if committed in accordance with the parties' intentions; and
- a party to the agreement, whether directly or via an agent, did anything in England and Wales regarding formation of the agreement before its formation, became a party to it in England and Wales, or did or omitted anything in England and Wales pursuant to the agreement.[67]

Where those conditions are satisfied, the prosecutor may pursue conspiracy charges under section 1A, referring to the offence as being a conspiracy to commit the underlying substantive offence (e.g., drug trafficking or people smuggling)[68] but for the fact that it was not triable in England and Wales.[69]

Similarly, the Fraud Act 2006 has expressly broad extraterritorial application.[70] Put simply, where any element of a statutory fraud offence[71] occurs within England and Wales, the court will have jurisdiction to try a defendant whether or not he or she was in the jurisdiction at any material time, and whether or not he or she was a British citizen at the time.

28.7.3 Inchoate offences

Separately, practitioners should not overlook the inchoate offences of encouraging or assisting others in the commission of offences. The Serious Crime Act 2007 includes statutory inchoate offences (under sections 44 to 46) of encouraging or assisting the commission of offences; these have extraterritorial application in certain circumstances.[72]

66 Inserted by the Criminal Justice (Terrorism and Conspiracy) Act 1998, s.5.

67 s.1A(1) to (5), Criminal Law Act 1977.

68 Respectively, *R v. Welsh (Christopher Mark)* [2015] EWCA Crim 1516, and *R v. Sophia Patel* [2009] EWCA Crim 67.

69 s.1A(6), Criminal Law Act 1977.

70 Part 1 of the Criminal Justice Act 1993 as amended by the Fraud Act 2006 (Schedule 1).

71 Being fraud by false representation (s.2), fraud by failing to disclose information (s.3), or fraud by abuse of position (s.4 Fraud Act 2006).

72 Through operation of s.52 of, and the conditions specified in Schedule 4 to, the Serious Crime Act 2007.

Where a person within England and Wales knows or believes that what is anticipated might occur wholly or partly in a place outside the jurisdiction, he or she will be liable under the Serious Crime Act 2007 if the anticipated offence would be triable in England if it were committed abroad or the anticipated conduct would amount to an offence under the local law of that other state.[73] Where that person is also outside the jurisdiction at the time of encouraging or assisting the anticipated offence, he or she will be liable under sections 44 to 46 if the person would otherwise be triable within England and Wales, for example on the basis of his or her British citizenship.[74]

Mutual legal assistance, cross-border production and the extraterritorial authority of UK enforcement agencies 28.8

Mutual legal assistance (MLA) allows a state to seek co-operation from another state in the investigation or prosecution of criminal offences via a formal letter of request. MLA is generally used when the enquiries require coercive means.[75] MLA is generally not appropriate if the material can be obtained directly via law enforcement co-operation for intelligence purposes or if the material otherwise is admissible in that form.

The framework governing the United Kingdom's approach to MLA is contained in a number of instruments, primarily the Crime (International Co-operation) Act 2003 (CICA), the European Convention on Mutual Legal Assistance in Criminal Matters 2000, and various bilateral and multilateral treaties (for example, with the United States in 1994, with Brazil in 2005 and with India in 1995). The UK Home Office Central Authority[76] is primarily tasked with receiving, and acceding to, MLA requests.[77]

Outgoing MLA requests (i.e., those from the United Kingdom to a foreign state) seeking evidence must be issued by a court or a designated prosecuting authority.[78] The MLA request can only be issued if it appears to the court or

73 Paras. 1 and 2 of Schedule 4, Serious Crime Act 2007.

74 For a discussion of this extraterritorial application, see the judgments in *R (Khan) v. Foreign Secretary*, regarding allegations that British intelligence officers committed offences under ss.44 to 46 of the SCA when they passed location information to agents of the United States Government for use in missile strikes by drone aircraft targeting individuals in Pakistan. *R (Khan) v. Secretary of State for Foreign and Commonwealth Affairs* [2014] EWCA Civ 24; and at first instance at [2012] EWHC 3728 (Admin). Ultimately, however, the claim did not continue because the court refused permission to proceed as the case would inevitably risk judicial condemnation of the actions of a foreign sovereign state.

75 While MLA is used for gathering and exchanging information, and requesting and providing assistance in obtaining evidence located abroad, extradition is the legal process by which an individual is transferred from one state to another for the purposes of being tried or serving a sentence already imposed. The Extradition Act 2003 sets out the UK extradition legal framework

76 If the request relates to tax and fiscal customs matters, the competent authority is HMRC.

77 There are exceptions such as EU freezing orders for property, which need to be sent directly to the relevant UK prosecuting authority.

78 The Director and any designated member of the Serious Fraud Office, the Financial Conduct Authority and the Bank of England are examples of designated prosecuting authorities.

designated prosecuting authority that an offence has been committed or there are reasonable grounds for suspecting that an offence has been committed or proceedings in respect of the offence have been instituted by the designated prosecuting authority, or the offence is being investigated.[79] The request must relate to the obtaining of evidence for use in the proceedings or investigation.[80] The defence can also apply for an MLA request once criminal proceedings have begun.[81] The usual policy for central or executing authorities is to keep the MLA request confidential and not to share its content beyond government departments, agencies, the courts or enforcement agencies.[82]

Evidence obtained from or by the United Kingdom pursuant to an MLA request cannot be used for any purpose other than that specified in the request without consent of the foreign authority.

In practice, persons subject to a request from a foreign authority, whether formal or informal, should ensure that they do not disclose material that is legally privileged, and ensure they take all appropriate steps to protect their rights under UK law, including as to the privilege against self-incrimination. For example, one method of MLA to foreign states is to compel witnesses to attend court.[83] Importantly, however, a witness cannot be compelled to give evidence where he or she could not otherwise be compelled to testify under either UK law or that of the requesting state.[84]

Furthermore, in the appropriate case, there is scope for judicial review of the UK authorities' response to a letter of request (LOR) from a foreign authority. In *R (on the application of Soma Oil and Gas Ltd) v. Director of the SFO*,[85] the High Court made clear that judicial review challenges to investigation decisions by authorities should be very rare, and only pursued in exceptional circumstances.[86] However, it does remain open to individuals subjected to a LOR to seek protection; the court noted: 'A balance must be struck between the public interest in international cooperation in investigating and prosecuting serious crime and the rights of the individual . . . . Though such challenges are not at all to be encouraged . . . they would dovetail well with the statutory and treaty regime *provided* their focus was upon compliance with the CICA and treaty conditions for the making of a LOR.'[87]

79 s.7(5), CICA 2003.

80 s.7(2)), CICA 2003.

81 s.7(1)(b) and (3)(c), CICA 2003.

82 In *Blue Holdings (1) Pte Ltd and another v. National Crime Agency* [2016] EWCA Civ 760, the appellant succeeded in inspecting an MLA request from the US Department of Justice to the National Crime Agency following the court's balancing exercise between the right to inspect a document in proceedings and an enforcement authority's claim to confidentiality.

83 s.15 CICA 2003.

84 Schedule 1 CICA 2003.

85 [2016] EWHC 2471.

86 *R (on the application of Unaenergy Group Holdings Pte Ltd and others) v. Director of the SFO* [2017] EWHC 600 (Admin) at para. 34 (iii) (*per* Gross LJ).

87 Ibid. at para. 35 (original emphasis).

In cases of concurrent or overlapping jurisdiction, prosecutors are encouraged to meet with their counterparts from overseas to discuss the relevant factors, such as the location and interests of witnesses and whether the prosecution can be appropriately split into separate cases. Where a case touches on issues of US jurisdiction, which has wide extraterritorial application, the UK prosecutor will need to consider the Attorney General's long-standing agreement with the US Department of Justice, and the related guidance (January 2007), which requires consultation and regular liaison from the outset of a relevant investigation.

Mutual legal assistance is not, of course, the only avenue for UK authorities to extend their information-gathering overseas. In February 2019, the Court of Appeal decided the case of *Jimenez*.[88] The Court held that Her Majesty's Revenue and Customs (HMRC) was entitled to serve an 'information notice'[89] on a British individual resident overseas to obtain information about his tax position. Mr Jimenez, a UK national resident in the United Arab Emirates, challenged service of that notice at his address in Dubai. HMRC had served the notice as part of its investigation into Mr Jimenez's tax affairs. In 2017, the High Court quashed the notice on the basis that Schedule 36 of the Finance Act 2008 was silent as to its extraterritorial effect. The Court of Appeal subsequently overturned that decision.

In the leading judgment for the Court of Appeal, Lord Justice Patten noted that the purpose of Schedule 36 was to prevent tax evasion, which is often cross-border in nature, and that the subject matter of the legislation identifies a sufficient jurisdictional nexus to the recipient of the notice (a UK taxpayer). Set against that context, Patten LJ noted the strong public policy reasons for conferring effective investigatory powers on HMRC, and also noted the absence of any express restriction on the geographical effect of the statute. Accordingly, the Court held that Parliament intended that specific information-gathering power should be available for investigating the UK tax position of relevant persons resident overseas. The Court also dismissed Mr Jimenez's argument that HMRC's conduct amounted to an exercise of UK official acts in the territory of another sovereign state. The Court held that service of the information notice did not seek to impose any criminal liability on a foreign national, and did not offend against the territorial sovereignty of the United Arab Emirates. Interestingly, Patten LJ noted that:

> *[A]nd the more recent decision[s] of the Supreme Court in* Bilta *and the Divisional Court in* KBR *confirm that the jurisdiction to serve a notice requiring the provision of information from a person resident abroad or even to impose liability on the recipient will not raise eyebrows where they serve to protect a sufficient national interest. In my view, the present case falls squarely within that category of case.*[90]

88 *R (on the application of Tony Michael Jimenez) v. First Tier Tax Tribunal (Tax Chamber) and HMRC* [2019] EWCA Civ 51.

89 Pursuant to para. 1 of Schedule 36 to the Finance Act 2008.

90 *R (on the application of Tony Michael Jimenez) v. First Tier Tax Tribunal (Tax Chamber) and HMRC* [2019] EWCA Civ 51 at para. 49.

28.8.1 Requests from within the European Union

Customarily much of the cross-border co-operation between authorities is informal, relying on established relationships whether directly between states or through organisations such as Interpol and Europol.[91] More recently, however, the European Union has embarked on a programme of reform, resulting in the European investigation order (EIO)[92] and in the proposed European production and preservation orders (EPOs). Although the United Kingdom has chosen to opt out of the proposals on EPOs, it has recently passed the Crime (Overseas Production Orders) Act 2019, which allows the courts to make orders similar to EPOs and enables law enforcement to obtain electronic data directly from an overseas communications service provider.

See Section 28.8.2

The purpose of the EIO is to make it easier for authorities in one Member State to obtain evidence from others through the mutual recognition principle. In contrast to MLA, following a validly issued EIO, a Member State must conduct the investigative measures specified by the order (subject to certain exceptions). Those measures may include the transfer of prisoners for the purposes of investigations, the hearing of witnesses by video link and covert investigation. An EIO may only be issued where there is 'dual criminality' in the receiving and executing countries. Broad exceptions to this principle (including offence categories such as terrorism, and human trafficking) that mirror the exceptions in the current scheme, exist however.

See Chapter 17 on individuals in cross-border proceedings

On receipt of an EIO, a participating Member State will have 30 days to decide whether to recognise and execute it. If the EIO is recognised, the request should be completed within 90 days, although extensions are permissible.

To apply for an EIO, an investigator in England and Wales must do so either to a 'designated public prosecutor', or by applying to a magistrates' court or the Crown Court, depending on the type of investigative measure sought. Defendants in criminal proceedings may also apply for an EIO from a judicial authority (any justice of the peace or judge). Irrespective of who is making the application, the public prosecutor or judicial authority must be satisfied that an offence has been committed, or there are reasonable grounds for suspecting that an offence has been committed, and proceedings have begun in respect of the offence, or it is being investigated.

At the time of writing, it is unclear how the EIO regime will work in the United Kingdom after Brexit, if at all. On 15 January 2019, the UK government published the draft Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (Exit Regulations), which address the relevant consequences of the United Kingdom leaving the European Union without a deal. The Exit Regulations seek to revoke the European Investigative Order Directive, including consequential amendments to British legislation, meaning that the United Kingdom would lose

91 For example, see the NCA website regarding its international co-operation. For a discussion of the European arrest warrant, see chapter 17 on individuals in cross-border investigations.

92 Directive 2014/41/EU was implemented in England and Wales by the Criminal Justice (European Investigation Order) Regulations 2017, which came into force on 31 July 2017.

European co-operation measures with regards to EIOs. Recently, one of the country's most senior police officers, the Assistant Commissioner of the Metropolitan Police, has acknowledged that safety and security will suffer from a no-deal Brexit, stating that certain systems and tools available through the EU were developed for a good reason. According to that officer, the loss of those tools would create 'an immediate risk that people could come to this country [the UK] who were serious offenders, either wanted or still serial and serious offenders committing crimes in this country, and we would not know about it.'[93]

Brexit 28.8.2

On 17 April 2018, the European Commission published its proposals for EPOs.[94] Unlike EIOs, EPOs will specifically target electronic evidence and would enable judicial authorities to receive electronic data from service providers within 10 days, and within six hours in an emergency. A preservation order would enable a judicial authority to require a service provider to preserve data, which could subsequently be obtained via MLA and an EIO or an EPO. The government has decided as of October 2018 against opting into the EU proposal for a legislation on the use of EPOs for cross-border access to electronic evidence in criminal matters.[95] The Crime (Overseas Production Orders) Act 2019 gives law enforcement agencies and prosecutors the power to obtain electronic data directly from an overseas communications service provider. The government has stated that this will be subject to robust judicial oversight, and that there exist statutory protections for legally privileged or journalistic material. The United Kingdom is also currently negotiating a data access agreement with the United States. Given broader uncertainties, at the time of writing, regarding Brexit and the new UK government, this remains an area for practitioners to watch.

Extradition and the European arrest warrant 28.8.3

Currently, the Extradition Act 2003 sets out the relevant UK legal framework. Extradition between EU Member States is governed by the European arrest warrant (EAW), which is based on principles of mutual trust and aims for speedy extradition proceedings.

After Brexit, however, the United Kingdom will need new arrangements with EU Member States to maintain appropriate degrees of co-operation. A return to the previous regime, under the 1957 Council of Europe Convention on Extradition, appears to be the default position and will inevitably lead to delays.

93 Vikram Dodd, 'Brexit: no deal would harm UK security, senior officer warns', *The Guardian*, 7 August 2019 (https://www.theguardian.com/uk-news/2019/aug/07/no-deal-brexit-would-harm-uk-security-senior-officer-warns), accessed 19 September 2019.

94 http://europa.eu/rapid/press-release_IP-18-3343_en.htm, accessed 19 September 2018.

95 Opt-in Decision on the Proposal of the European Parliament and the Council on European Production Orders and European Preservation Orders for cross-border access to electronic evidence in criminal matters: Written statement – HCWS1024, 22 October 2018.

Indeed, the House of Lords concluded in a report[96] that '[f]alling back on the 1957 Council of Europe Convention on Extradition would significantly slow down extradition proceedings, since it would mean going back to making routine extradition requests – as well as resolving disputes about extradition requests – through diplomatic channels.'[97]

Brexit is unlikely to affect extradition arrangements with category 2 territories as designated by the Extradition Act 2003 (countries with international extradition arrangements other than the EAW, such as the United States).

28.8.4 Economic Crime Plan, 2019–2022

In July 2019, the government published its Economic Crime Plan, 2019–2022 (the Plan).[98] Continuing a theme from recent years, the Plan emphasises the need for the public and private sectors to work together to help the United Kingdom counter all forms of economic crime. This is underpinned by seven strategic objectives, which include improving systems for transparency of ownership of legal entities and legal arrangements, and delivering an ambitious international strategy to enhance security, prosperity and global influence.

Aimed at countering money laundering through the UK real estate market, the Plan seeks, among other things, to improve transparency of overseas ownership of British property by finalising legislation that will establish a public register of the beneficial owners of overseas foreign companies that hold UK property.[99] The register is described as being the first of its type in the world and is proposed to be operational in 2021.

The Plan also describes an intention to strengthen UK law enforcement agencies' capability to prosecute bribery and corruption. Increased funding is proposed for the International Corruption Unit at the NCA and for the Crown Prosecution Service, to enable them to recover and return assets stolen from developing countries by corrupt individuals and pursue UK companies and nationals who engage in bribery and corruption in developing countries.

The Plan recognises that domestic and international action are mutually supporting. To enhance overseas capabilities, the Plan aims to:

- coordinate networks of policy expertise, including the development of a new hybrid platform (the International Centre of Excellence), which combines public, private and academic expertise to tackle illicit financing in existing and emerging regional and global financial centres;

96 European Union Committee, 'Brexit: judicial oversight of the European Arrest Warrant', (6th Report of Session 17–19, HL Paper 16).

97 Ibid., at para. 73.

98 Economic Crime Plan, 2019-22, July 2019 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf), accessed 19 September 2019.

99 Draft Registration of Overseas Entities Bill 2019.

- embed staff in high priority jurisdictions to facilitate joint responses to shared threats; and
- improve co-operation between UK law enforcement agencies and their international counterparts.

The Plan acknowledges that the United Kingdom has made significant progress in recognising and responding to the threat from economic crime through world-leading reforms, including through the creation of the National Economic Crime Centre, which was established in October 2018 to substantially improve the response to tackling serious and organised crime. It brings together law enforcement and justice agencies, government departments, regulatory bodies and the private sector to 'protecting the public and safeguarding the prosperity and reputation of the UK as a financial centre'.[100]

100 https://nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre, accessed 19 September 2019.

29

Extraterritoriality: The US Perspective

James P Loonam and Conor Reardon[1]

29.1 Extraterritorial reach of US laws

Investigations conducted by US prosecutors and regulators often concern conduct outside the United States and involve evidence located abroad. The two questions of whether US law applies to the conduct under investigation and whether US authorities can compel the production of evidence located abroad are of significant importance to practitioners. As to the first question, in a series of civil cases, the United States Supreme Court has reasserted a presumption against the extraterritorial application of US statutes.[2] What this means is that lower US courts have been instructed to assume that US law applies only to conduct that takes place within the borders of the United States unless the particular law explicitly states it has exterritorial application. In practice, this presumption is an important but limited check on US prosecutors' and regulators' powers to investigate and bring cases involving foreign conduct. Even limited contacts with the United States, such as the use of the US wires or financial system, may bring related conduct that takes place outside the United States within the domestic purview of certain US laws. Courts look to the statute's 'focus'[3] to determine whether a case involves a domestic application of a statute:

1 James P Loonam is a partner, and Conor Reardon is an associate, at Jones Day.

2 *Morrison v. Nat'l Australia Bank, Ltd.*, 561 U.S. 247 (2010); *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108 (2013); *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016).

3 *Morrison v. Nat'l Australia Bank, Ltd.*, 561 U.S. 247 (2010); *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016).

> *If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in US territory.*[4]

In recent years, lower courts have grappled with this issue of determining the focus of various statutes case by case and have not always reached consistent results. This chapter will address the recent jurisprudence in this area, focusing on statutes that are most commonly invoked to reach overseas conduct. As to the second question, US prosecutors often seek to obtain evidence located overseas during the course of investigations. This chapter will address the muscular stance recently taken by prosecutors to obtain evidence located overseas from non-US entities and the support this approach has found in the courts to date.[5]

Securities laws 29.2

The Securities Exchange Act of 1934 (the Exchange Act) regulates domestic securities markets and transactions. Its general anti-fraud provision, Section 10(b), along with accompanying SEC Rule 10b-5, prohibits fraud in connection with the purchase or sale of securities. The Exchange Act and its associated rules are enforced civilly by the SEC (as well as through private actions) and criminally by the US Department of Justice (DOJ). Much recent extraterritoriality litigation – including the Supreme Court's landmark decision in *Morrison v. Nat'l Australia Bank Ltd*[6] – has involved the securities laws.

The Morrison decision 29.2.1

Some forty years before *Morrison*, the Second Circuit developed an approach to extraterritoriality in the securities fraud context that would be adopted (albeit with variation) by many other courts of appeals.[7] Under this 'conduct and effects' test, the court determined the extraterritorial reach of the securities laws in a given case by asking (1) 'whether the wrongful conduct had a substantial effect in the United States or upon United States citizens', and (2) 'whether the wrongful conduct occurred in the United States'.[8] Other circuits adopted related (though not identical) tests.[9] Whatever the precise formulation, the conduct-and-effects

4 *RJR Nabisco*, 136 S. Ct. at 2101.

5 See, e.g., *In re: Sealed Case*, No. 19-5068 (D.C. Cir. 6 August 2019).

6 561 U.S. 247 (2010).

7 See *Leasco Data Processing Equip. Corp. v. Maxwell*, 468 F.2d 1326 (2d Cir. 1972); *Schoenbaum v. Firstbrook*, 405 F.2d 200 (2d Cir. 1968).

8 *Morrison*, 561 U.S. at 257 (quoting *SEC v. Berger*, 322 F.3d 187, 192–93 (2d Cir. 2003)).

9 See id. at 259 (collecting cases).

approach required a fact-intensive, case-specific inquiry calculated to reveal whether Congress would have wanted United States law to apply had it considered the matter.[10]

In *Morrison*, the Supreme Court rejected this long-standing test. The Court criticised the notion that congressional silence on the extraterritorial scope of Section 10(b) gave judges licence to 'determine what Congress would have wanted'.[11] It added that the imprecise conduct-and-effects approach was inconsistent in application and yielded unpredictable results.[12] The proper approach, the majority held, was to apply the presumption against extraterritoriality in all cases.[13] Because Section 10(b) lacked 'a clear statement of extraterritorial effect', it applied only domestically.[14]

The Court went on to describe the domestic scope of Section 10(b). The statute's focus is not merely deceptive conduct, but deceptive conduct 'in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered'.[15] Therefore, Section 10(b) applies only to 'transactions in securities listed on domestic exchanges, and domestic transactions in other securities'.[16]

In explaining the territorial reach of Section 10(b), the Court upset existing case law in another respect. Many courts had considered a statute's extraterritorial scope to raise a question of subject-matter jurisdiction.[17] Not so, wrote the majority: to 'ask what conduct Section 10(b) reaches is to ask what conduct Section 10(b) prohibits', which is not a question of adjudicative authority but 'a merits question'.[18]

29.2.2 Post-Morrison developments

In *Morrison*, the Court announced that its new approach was (unlike the conduct-and-effects standard) a 'clear test' that could be predictably applied.[19] Nonetheless, lower courts have wrestled with a number of questions that *Morrison* did not answer.

One fundamental issue arises not from any lack of clarity in *Morrison*, but from Congress's apparent response to the decision. Days after *Morrison* came down, a joint congressional committee finalising the proposed Dodd-Frank Act published a final version of the bill, which would be enacted less than a month later.[20] That version (and the enacted law) included a provision, Section 929P,

10 Id. at 259–60.
11 Id. at 260.
12 Id.
13 Id.
14 Id. at 265.
15 Id. at 266–67 (quoting 15 U.S.C. § 78j(b)).
16 Id.
17 Id. at 253–54.
18 Id. at 254.
19 Id. at 269.
20 Pub. L. No. 111-203, 124 Stat. 1376 (2010).

that appears calculated to abrogate *Morrison* in the context of SEC and criminal actions. It amends the jurisdictional section of the Exchange Act by providing that district courts 'shall have jurisdiction' over such actions involving 'conduct within the United States that constitutes significant steps in furtherance of the violation' or 'conduct occurring outside the United States that has a foreseeable substantial effect within the United States'.[21] The legislator who had drafted the provision, Representative Paul Kanjorski, stated that its purpose 'was to make clear that the antifraud provisions apply extraterritorially in enforcement actions'.[22]

The intent behind Section 929P seems clear enough, but *Morrison* explicitly held that the question of a statute's extraterritorial application is a merits question, not a jurisdictional question. Section 929P speaks only to jurisdiction and leaves untouched the substantive anti-fraud provisions of the Exchange Act. Faced with this conflict between contextual evidence of congressional intent and plain text, several courts have sidestepped the issue.[23] But in 2019, the Tenth Circuit became the first court of appeals to directly confront the question. The court prioritised 'context and historical background' – particularly Congress's inability to respond to *Morrison*'s jurisdiction/merits holding in the days between the decision and reporting of the final bill – to hold that Section 929P abrogated *Morrison* and that 'the substantive antifraud provisions should apply extraterritorially when the statutory conduct-and-effects test is satisfied.'[24] Whether other courts of appeals will embrace the Tenth Circuit's conclusion remains to be seen.

In addition to this basic question of *Morrison*'s vitality outside the context of private actions, courts have addressed a number of issues regarding its application. The first prong of *Morrison*'s transactional test permits actions based on 'transactions in securities *listed* on domestic exchanges'.[25] In 2014, the Second Circuit considered whether this formulation permitted a 'foreign-cubed' claim – foreign institutional investors suing foreign banking defendants over shares purchased on a foreign exchange – because those shares were cross-listed on the New York Stock Exchange.[26] The court acknowledged that the plaintiffs' 'listing theory' comported with *Morrison*'s language 'taken in isolation', but concluded that, 'read as a whole', *Morrison* made clear that domestic application of the Exchange Act requires that the shares in question be purchased, not just listed, on a domestic exchange.[27]

21 15 U.S.C. § 78aa(b).

22 *SEC v. Scoville*, 913 F.3d 1204, 1218 (10th Cir.2019), cert. denied, 18-1566 (4 November 2019).

23 See, e.g., *SEC v. Chicago Convention Ctr., LLC*, 961 F. Supp. 2d 905, 911–17 (N.D. Ill. 2013) ('The plain language of Section 929P(b) and its placement in the jurisdictional section of the Exchange Act indicate that it may be jurisdictional. It is unclear, however, whether the Court's analysis should stop there because it is possible that this interpretation would create superfluity or contradict the legislative intent. The Court need not resolve this complex interpretation issue, however, because . . . under either the *Morrison* "transactional" inquiry or the allegedly revived "conduct and effects test," the SEC's Complaint survives the present motion to dismiss.').

24 *Scoville*, 913 F.3d at 1218.

25 *Morrison*, 561 U.S. at 267 (emphasis added).

26 *City of Pontiac Policemen's & Firemen's Ret. Sys. v. UBS AG*, 752 F.3d 173, 179–80 (2d Cir. 2014).

27 Id. at 180–81.

Courts have also addressed just what qualifies as a domestic exchange. One district court held in 2011 that *Morrison*'s first prong reaches securities traded on domestic over-the-counter markets, reasoning that 'transactions on the domestic over-the-counter market are as imbued with our national interest as trades on national exchanges.'[28] But that decision appears to be an outlier. Other courts have concluded that over-the-counter transactions may qualify under *Morrison*'s second prong (as domestic transactions in other securities), but do not occur on exchanges.[29]

Morrison's second prong has likewise received attention from litigants and courts. In 2012, the Second Circuit held that a securities transaction is domestic under *Morrison* if (1) 'the purchaser incurred irrevocable liability within the United States to take and pay for a security;' (2) 'the seller incurred irrevocable liability within the United States to deliver a security;' or (3) 'title to the shares was passed within the United States.'[30] Under the 'irrevocable liability' test, the court must identify 'the point at which the parties obligated themselves to perform what they had agreed to perform even if the formal performance of their agreement is to be after a lapse of time'.[31] What matters is not where the 'contract is said to have been executed' as a matter of contract law, but 'where, physically, the purchaser or seller committed him or herself'.[32] The Second Circuit's approach has met generally with approval and has been expressly adopted by the Third and Ninth

28 *SEC v. Ficeto*, 839 F. Supp. 2d 1101, 1108 (C.D. Cal. 2011); see id. at 1108–14.

29 See, e.g., *Stoyas v. Toshiba Corp.*, 896 F.3d 933, 945–47 (9th Cir. 2018); *United States v. Georgiou*, 777 F.3d 125, 134–35 (3d Cir. 2015); *In re Volkswagen 'Clean Diesel' Marketing, Sales Practices, and Prods. Liab. Litig.*, Nos. 15-cv-6167, 15-cv-6168, 16-cv-190, 16-cv-184, 2017 WL 66281, at *3–4 (N.D. Cal. 4 January 2017).

30 *Absolute Activist Value Master Fund Ltd. v. Ficeto*, 677 F.3d 60, 68–69 (2d Cir. 2012).

31 Id. at 68.

32 *United States v. Vilar*, 729 F.3d 62, 77 n.11 (2d Cir. 2013). Notwithstanding this focus on where, 'physically', the parties committed themselves, the Second Circuit has also stated that '[t]he location . . . of the buyer, seller, or broker will not necessarily establish the situs of the transaction.' *In re Petrobas Sec.*, 862 F.3d 250, 262 (2d Cir. 2017). The recent case of *United States v. Boustani* implicated this tension. The DOJ initially contended that its indictment alleged domestic transactions because 'United States investors purchased [the relevant securities] while physically present in the United States.' Memorandum in Opposition 15–17, *United States v. Boustani*, No. 18-cr-681-WFK (E.D.N.Y. 22 July 2019), ECF No. 113. The defendant argued that this fact alone did not establish domesticity, and that the relevant transactions occurred abroad because they were settled and cleared in Europe. Memorandum of Law in Support of Motion to Dismiss 19–24, *United States v. Boustani*, No. 18-cr-681-WFK (E.D.N.Y. 21 June 2019), ECF No. 98. Before the Court decided the issue, the government obtained a superseding indictment, which alleged that 'investors in the United States incurred irrevocable liability in the United States by purchasing the [securities] while physically present in the United States.' Supplemental Memorandum in Opposition 14-15, *United States v. Boustani*, No. 18-cr-681-WFK (E.D.N.Y. 13 Sept 2019), ECF No. 166. The defendant's motion to dismiss the indictment was denied. Decision & Order, *United States v. Boustani*, No. 18-cr-681-WFK (E.D.N.Y. 3 Oct 2019), ECF No. 231. On 2 December the jury acquitted the defendant on all counts. The defence had argued that 'the US is not the world's policeman'. Three jurors later told press that they could not see 'how federal prosecutors in Brooklyn had the authority to prosecute crimes that hadn't occurred in their jurisdiction'. Patricia Hurtado, 'Salesman Cleared in US$2 Billion African Scam in Blow to US' Bloomberg (2 December 2019),

Circuits.[33] Determining whether irrevocable liability was incurred, or title passed, in the United States requires analysis of 'factual allegations concerning contract formation, placement of purchase orders, passing of title, and the exchange of money'.[34] Given the varied and complex nature of modern transactions in securities, the moment of irrevocable commitment (or passing of title) will not always be obvious.[35]

Finally, two courts of appeals disagree about a fundamental aspect of *Morrison*'s holding: is a domestic transaction in a security (or a transaction in a security listed domestically) merely necessary for application of the Exchange Act, or is it both necessary and sufficient? In *Parkcentral Global Hub Ltd v. Porsche Auto Holdings SE*,[36] the Second Circuit concluded that some domestic transactions are beyond the territorial reach of Section 10(b). The plaintiffs in *Parkcentral* were international hedge funds that entered securities-based swap agreements in the United States.[37] These instruments were pegged to the price of Volkswagen shares, but the shares themselves were traded only on foreign exchanges, and the foreign defendant (which had allegedly engaged in fraud, primarily in Germany, affecting the price of shares) was not a counterparty to any of the agreements.[38] The court acknowledged that the relevant transactions had occurred in the United States, but nonetheless concluded that the case was extraterritorial. If the suit proceeded, 'it would permit the plaintiffs, by virtue of an agreement independent from the reference securities, to hale the European participants in the market for German stocks into US courts and subject them to US securities laws.'[39] This would incompatible with *Morrison*.

In *Stoyas v. Toshiba Corp*, the Ninth Circuit disagreed. *Toshiba*, like *Parkcentral*, involved American depository receipts (ADRs), issued by United States depositary institutions without defendant Toshiba's formal participation and representing a beneficial interest in, not legal ownership of, Toshiba shares.[40] The plaintiffs alleged that Toshiba had engaged in fraud overseas, causing the value of its shares (and the value of plaintiffs' ADRs) to decrease. It appeared that plaintiffs had

available at https://www.bloomberg.com/news/articles/2019-12-02/privinvest-salesman-is-acquitted-of-defrauding-u-s-investors.

33 See *Stoyas*, 896 F.3d at 947–49; *Georgiou*, 777 F.3d at 137.

34 *Stoyas*, 896 F.3d at 949.

35 See *SEC v. Ahmed*, 308 F. Supp. 3d 628, 660–64 (D. Conn. 2018) (summarising cases applying the Second Circuit's standard in a variety of factual circumstances).

36 763 F.3d 198 (2d Cir. 2014).

37 Id. at 207.

38 Id. at 206–08.

39 Id. at 214–17. After *Parkcentral*, some Second Circuit decisions distinguished or ignored the case, casting doubt on its continued relevance. See, e.g., *Giunta v. Dingman*, 893 F.3d 73, 82 (2d Cir. 2018); *Myun-Uk Choi v. Tower Research Capital LLC*, 890 F.3d 60, 66 (2d Cir. 2018). But in 2019, in a case arising under the Commodity Exchange Act, the court both reaffirmed *Parkcentral* and extended it to that new statutory context. See *Prime Int'l Trading, Ltd. v. BP P.L.C.*, --- F.3d ----, 2019 WL 4062219, at *6–8 (2d Cir. 29 August 2019).

40 *Stoyas*, 896 F.3d at 940–41.

purchased the ADRs in the United States.[41] But Toshiba argued that the case was nonetheless extraterritorial. As in *Parkcentral*, there was 'no connection between Toshiba and the Toshiba ADR transactions', making the dispute so overwhelmingly foreign as to require dismissal.[42] The Ninth Circuit disagreed. The court wrote that *Parkcentral* was distinguishable on several grounds, but that, in any event, it was wrongly decided: the Second Circuit's approach replaced *Morrison*'s bright-line transactional test with an undefined standard asking whether (notwithstanding a domestic transaction) a case was 'too foreign' for US adjudication.[43]

The Supreme Court declined to review the Ninth Circuit's *Stoyas* decision, leaving the circuit conflict unresolved. As it stands, the practical importance of the disagreement is unclear. The Ninth Circuit indicated that in the unusual circumstances present in *Parkcentral* and *Stoyas* – namely a foreign defendant drawn into a US lawsuit based solely on domestically traded derivative instruments – other elements of Section 10(b), such as the requirement that fraud be 'in connection with' the purchase or sale of a security, might preclude liability.[44]

29.3 Criminal versus civil cases

In *Morrison*, the Supreme Court described the applicability of the presumption against extraterritoriality in unequivocal terms: 'Rather than guess anew in each case, we apply the presumption in all cases.'[45] That blanket pronouncement sits uneasily with *United States v. Bowman*,[46] a 1922 decision holding that the presumption is inapplicable in certain classes of criminal cases. Neither *Morrison* nor any of the Court's other recent extraterritoriality decisions arose in the criminal context, creating uncertainty about how the Court's aggressive application of the presumption translates to criminal prosecutions.

The defendants in *Bowman* schemed to defraud a government-owned company, acting on the high seas and in Brazil.[47] The Court acknowledged the presumption against extraterritoriality and stated that it applied to '[c]rimes against private individuals or their property, like assaults, murder, burglary, larceny, robbery, arson, embezzlement, and frauds of all kinds'.[48] But, the Court reasoned, 'the same rule of interpretation should not be applied to criminal statutes which are, as a class, not logically dependent on their locality for the government's jurisdiction, but are enacted because of the right of the government to defend itself against

41 Id. at 949.
42 Id. at 949.
43 Id. at 950.
44 Id. at 950–52.
45 *Morrison*, 561 U.S. at 261.
46 260 U.S. 94 (1922).
47 Id. at 95–97.
48 Id. at 98.

obstruction, or fraud wherever perpetrated.'[49] In such cases, Congress need not speak clearly for its statute to apply extraterritorially, for it has allowed it 'to be inferred' from the 'nature' of the offence.[50]

By its terms, the *Bowman* exception was drawn narrowly.[51] But in the decades that followed, the courts of appeals 'applied *Bowman* . . . with varying degrees of liberality',[52] and many courts held *Bowman* applicable (and the presumption against extraterritoriality inoperative) in circumstances well removed from 'criminal statutes . . . enacted because of the right of the government to defend itself against obstruction, or fraud wherever perpetrated'.[53] For example, some courts drew on *Bowman*'s reference to the nature of the crime to exempt whole classes of criminal statutes that frequently involve transnational conduct or effects, such as 'immigration . . . , sex tourism and human trafficking, and drug trafficking'.[54]

The Court's reinvigorated commitment to the presumption against extraterritoriality suggests that, in an appropriate case, it might be willing to revisit *Bowman*. In the meantime, lower courts have not been willing to conclude that *Bowman* has been impliedly overruled.[55] The government has read *Bowman* broadly to argue that cases like *Morrison* and *RJR Nabisco* simply do not apply in criminal matters. Lower courts have not been receptive to that argument either.[56] Instead, the question in lower courts has been the extent of the *Bowman* exception in light of the Court's recent extraterritoriality decisions. Many have applied the presumption in criminal cases while acknowledging that there is tension between *Morrison* and *Bowman* or, at a minimum, explaining that *Morrison* highlights the need to confine *Bowman*'s exception to narrow limits.[57]

---

49 Id.

50 Id.

51 Id. at 98–99.

52 *United States v. McVicker*, 979 F. Supp. 2d 1154, 1171 (D. Or. 2013).

53 *Bowman*, 260 U.S. at 98.

54 Zachary D Clopton, Bowman Lives: The Extraterritorial Application of U.S. Criminal Law After Morrison v. National Australia Bank, 67 N.Y.U. Ann. Surv. Am. L. 137, 169–70 (2011); see id. at 170 nn. 135–37 (collecting cases).

55 E.g., *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 91 n.5 (D.D.C. 2017), reconsideration granted in part on other grounds sub nom. *United States v. All Assets Held at Bank Julius, Baer & Co., Ltd.*, 315 F. Supp. 3d 90 (D.D.C. 2018).

56 See, e.g., *United States v. Vasquez*, 899 F.3d 363, 374 (5th Cir. 2018) (rejecting the 'puzzling position' that '*RJR Nabisco* does not apply to criminal cases'); *United States v. Vilar*, 729 F.3d 62, 72 (2d Cir. 2013) ('no plausible interpretation of *Bowman*' supported the government's argument that 'the presumption against extraterritoriality has no place in our reading of criminal statutes').

57 See, e.g., *Vasquez*, 899 F.3d at 373–74 & n.6; *Vilar*, 729 F.3d at 72–74; *All Assets*, 251 F. Supp. 3d at 91 n.5; *United States v. Abu Khatallah*, 151 F. Supp. 3d 116, 124–26 (D.D.C. 2015) (explaining that *Bowman* 'sits uneasily with *Aramco*, *Morrison*, and *Kiobel*'). But not all courts have embraced the idea that the Court's recent extraterritoriality cases bear on the *Bowman* exception. See, e.g., *United States v. Leija-Sanchez*, 820 F.3d 899, 901 (7th Cir. 2016) ('A decision such as *Bowman*, holding that criminal and civil laws differ with respect to extraterritorial application, is not affected by yet another decision showing how things work on the civil side [i.e., *Morrison*].').

However lower courts navigate the *Bowman–Morrison* tension as a general matter, *Morrison* appears to bear directly on the interpretation of 'hybrid' statutes, namely statutes that apply both criminally and civilly. As a rule, federal courts construe hybrid statutes consistently across applications, rather than interpret the same statute one way in criminal cases and another in civil cases.[58] *Morrison* makes clear that the presumption against extraterritoriality (1) applies universally in (at least) the civil context, and (2) is a rule of statutory construction.[59] Therefore, under *Morrison*, statutes capable of civil application should be construed using the presumption against extraterritoriality, generating an interpretation that applies perforce if the statute is also capable of criminal application. Indeed, as the Second Circuit held in *Vilar*, the statute construed in *Morrison* – Section 10(b) – is itself a hybrid statute and after *Morrison* lacks extraterritorial effect in both its civil and criminal dimensions.[60]

29.4 RICO

The Racketeer Influenced and Corrupt Organizations Act (RICO) prohibits engaging in 'a pattern of racketeering activity' in relation to an enterprise.[61] 'The statute defines "racketeering activity" to encompass dozens of state and federal offenses, known in RICO parlance as predicates.'[62] Violations of RICO's substantive prohibitions are subject to criminal prosecution and civil enforcement proceedings.[63] In addition, RICO creates an express private right of action for '[a]ny person injured in his business or property by reason of a violation of Section 1962'.[64]

See Chapter 26 on fines, disgorgement, etc.

58 See, e.g., *Leocal v. Ashcroft*, 543 U.S. 1, 12 n.8 (2004) ('[W]e must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context.'); *FCC v. Am. Broadcast Co.*, 347 U.S. 284, 296 (1954) ('There cannot be one construction for the Federal Communications Commission and another for the Department of Justice.'); *Carter v. Welles-Bowen Realty, Inc.*, 736 F.3d 722, 727 (6th Cir. 2013) ('A single statute with civil and criminal applications receives a single interpretation.'). Notwithstanding the Supreme Court's apparently clear statements on this matter, some cases contravene or call into question the rule of consistent interpretation. See, e.g., *United States v. Plaza Health Labs, Inc.*, 3 F.3d 643, 648 (2d Cir. 1993); see also *Babbitt v. Sweet Home Chapter of Communities for a Greater Oregon*, 515 U.S. 687, 704 n.18 (1995) (deferring to an agency interpretation of a law carrying criminal penalties, and suggesting that the rule of lenity had no application because the case arose in a civil context).

59 See *Vilar*, 729 F.3d at 74.

60 Id. ('[E]ven if it were the case that we do not generally apply the presumption against extraterritoriality to criminal statutes, Section 10(b) would still not apply extraterritorially in criminal cases. The reason is simple: The presumption against extraterritoriality is a method of interpreting a statute, which has the same meaning in every case.'); see *Vasquez*, 899 F.3d at 373 n.6 (applying *RJR Nabisco* to a criminal RICO case, and explaining that RICO 'is a hybrid statute authorizing criminal prosecution, civil enforcement, and private civil actions' (internal citations omitted)); see id. (collecting criminal RICO cases that apply *RJR Nabisco*).

61 *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2096–97 (2016); see 18 U.S.C. § 1962.

62 *RJR Nabisco*, 136 S. Ct. at 2096.

63 18 U.S.C. §§ 1963(a), 1964(a)–(b).

64 *RJR Nabisco*, 136 S. Ct. at 2097 (quoting 18 U.S.C. § 1964(c)).

The Supreme Court considered RICO's extraterritorial scope in *RJR Nabisco*, a civil action brought by the European Community and 26 of its Member States against defendants alleged to have 'participated in a global money-laundering conspiracy in association with various organized crime groups'.[65] The Court reached three significant conclusions. First, it held that RICO overcomes the presumption against extraterritoriality because certain predicates apply extraterritorially, 'a clear, affirmative indication that Section 1962 applies to foreign racketeering activity'.[66] But 'when a statute provides for some extraterritorial application, the presumption against extraterritoriality operates to limit that provision to its terms.'[67] Therefore, RICO applies extraterritorially 'only to the extent that the predicates alleged in a particular case themselves apply extraterritorially'.[68] Second, the Court held that – even where an alleged predicate offence applies extraterritorially – RICO's substantive prohibitions require 'proof of an enterprise that is "engaged in, or the activities of which affect, interstate or foreign commerce"' .[69] This necessary link to US commerce provides a further limit on RICO's extraterritorial scope. Third, the Court held that RICO's private right of action has no extraterritorial application, even in cases involving extraterritorial predicates.[70] 'A private RICO plaintiff therefore must allege and prove a domestic injury to its business or property.'[71]

A number of courts have applied *RJR Nabisco* in the context of criminal prosecutions.[72] In a criminal case, where the domestic-injury requirement applicable to private plaintiffs has no operation, extraterritorial application will turn on the reach of the alleged predicates and the nexus between the enterprise and US commerce.[73]

Wire fraud 29.5

The wire fraud statute, 18 USC Section 1343, prohibits wire transmissions 'in interstate or foreign commerce . . . for the purpose of executing' a scheme to defraud. Federal prosecutors have broadly applied this statute to reach a variety of fraudulent conduct. Questions of the extraterritoriality of the wire fraud statute arise not only in criminal prosecutions, but also in civil cases, particularly RICO suits in which wire fraud is alleged as a predicate act.

65 Id. at 2098.

66 Id. at 2102.

67 Id. (quoting *Morrison*, 561 U.S. at 265).

68 Id.

69 Id. at 2105 (quoting 18 U.S.C. § 1962(a)–(c)).

70 Id. at 2106.

71 Id.

72 See, e.g., *United States v. Vasquez*, 899 F.3d 363, 373 n.6 (5th Cir. 2018) (citing *United States v. Sitzmann*, 893 F.3d 811, 822 (D.C. Cir. 2018) (*per curiam*); *United States v. Ubaldo*, 859 F.3d 690, 700–01 (9th Cir. 2017); *United States v. Valenzuela*, 849 F.3d 477, 484–85 & n.3 (1st Cir. 2017); *United States v. Gasperini*, 729 F. App'x 112, 113–14 (2d Cir. 2018)).

73 See, e.g., *United States v. Hawit*, No. 15-cr-252-PKC, 2017 WL 663542, at *9–10 (E.D.N.Y. 17 February 2017).

Courts disagree about whether Section 1343 applies extraterritorially. In *United States v. Georgiou*,[74] the Third Circuit held that it does. The court relied on *dicta* from *Pasquantino v. United States*,[75] in which the Supreme Court stated that 'the wire fraud statute punishes frauds executed in "interstate or foreign commerce", so this is surely not a statute in which Congress had only "domestic concerns in mind".'[76] But the Second Circuit rejected that view in *European Community v. RJR Nabisco, Inc*.[77] The court acknowledged the *dicta* in *Pasquantino* but reasoned that it had been abrogated by *Morrison*, which held that 'a general reference to foreign commerce . . . does not defeat the presumption against extraterritoriality.'[78] After concluding that the statute had no extraterritorial application, however, the Second Circuit left unsettled the second step of the inquiry (i.e. the focus, and therefore the domestic reach, of Section 1343) by disclaiming any need to decide 'precisely how to draw the line between domestic and extraterritorial applications of the wire fraud statute'.[79] The court reasoned that the defendants were alleged to have satisfied each element of the statute through conduct in the United States; accordingly, 'wherever [the] line should be drawn', the case fell on the domestic side of it.[80]

After *European Community*, district courts – particularly district courts within the Second Circuit – struggled to define the kind and degree of domestic conduct necessary for application of the wire fraud statute. In *Laydon v. Mizuho Bank, Ltd*,[81] defendants acting abroad were alleged to have manipulated benchmark interest rates through fraudulent submissions to entities in London and Tokyo.[82] The court rejected the idea that mere use of the domestic wires in connection with the fraud was sufficient without proof that the scheme was managed from or directed to the United States.[83] Yet in *United States v. Hayes*,[84] another benchmark manipulation case, the court stated without qualification that using 'domestic wires to carry out [a] fraudulent scheme' is 'clearly sufficient' for domestic application. Some courts tried to explain this apparent divergence on the ground that *Laydon* was civil and *Hayes* criminal.[85] But the court in *United States v. Gasperini*,[86]

74 777 F.3d 125 (3d Cir. 2015).

75 544 U.S. 349 (2005).

76 Id. at 371–72 (internal citation omitted).This statement was made *obiter* in that the Court held that the case involved a domestic application of the statute. Id.

77 764 F.3d 129 (2d Cir. 2014), rev'd on other grounds sub nom. *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016).

78 Id. at 141 (quoting *Morrison*, 561 U.S. at 263).

79 Id. at 142.

80 Id.

81 No. 12-cv-3419-GBD, 2015 WL 1515487 (S.D.N.Y. 31 March 2015).

82 Id. at *1, *9.

83 Id. at *8–9.

84 99 F. Supp. 3d 409 (S.D.N.Y. 2015).

85 See *Sonterra Cap. Master Fund v. Credit Suisse Grp.*, 277 F. Supp. 3d 521, 581 (S.D.N.Y. 2017); see also *FrontPoint Asian Event Driven Fund, L.P. v. Citibank, N.A.*, No. 16-cv-5263-AKH, 2017 WL 3600425, at *15 (S.D.N.Y. 18 August 2017).

86 No. 16-cr-441-NGG, 2017 WL 2399693 (E.D.N.Y. 1 June 2017).

a criminal case, applied a *Laydon*-like analysis to hold that the focus of the wire fraud statute is 'the scheme to defraud', and that domestic application of Section 1343 requires 'a substantial amount of conduct in the United States' that is 'integral to the commission of the scheme'.[87]

After several years of confusion, the Second Circuit imposed a measure of order in *Bascuñán v. Elsaca*.[88] Bascuñán was a civil RICO case (with a wire fraud predicate) in which the plaintiff alleged that the defendant, acting abroad, had fraudulently used domestic wires to obtain funds from New York bank accounts.[89] The Second Circuit noted that the critical issue, the focus of the wire fraud statute 'for the purpose of the presumption against extraterritoriality [was] a question of first impression in [the] circuit'.[90] The court rejected the view that the wire fraud statute gives way unless the scheme to defraud is 'planned, managed, and directed' from the United States.[91] It reasoned that the focus of Section 1343 'is not merely a scheme to defraud, but more precisely the use of the . . . wires in furtherance of a scheme to defraud'.[92] The court went on to observe that the Supreme Court, and other courts of appeals, 'though not in the context of applying the presumption against extraterritoriality [had] described the focus' of the wire fraud statute in precisely those terms.[93] But not just any wire furthering a scheme would do. Because 'incidental' domestic conduct is not enough to trigger United States law, use of the wires 'must be essential' to, or 'a core component of', the scheme to defraud.[94] Applying this standard to the facts was straightforward, in that the defendant allegedly had used domestic wires to fraudulently 'transfer millions of dollars' out of domestic bank accounts – clearly a core component of the scheme.[95]

Bascuñán therefore goes some distance toward resolving the confusion that persisted after *European Community*. Still, open questions remain. In November 2019, the Second Circuit heard arguments regarding the application of *Bascuñán* to honest services fraud.[96] In addition, it remains to be seen whether other courts of appeals will follow *Bascuñán*. The Sixth and Ninth Circuits have reached the same basic conclusion, albeit in non-precedential opinions.[97] And (as the Second

87 Id. at *7–8; see also *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 103 (D.D.C. 27 April 2017) (applying the same test).

88 927 F.3d 108 (2d Cir. 2019).

89 Id. at 112–15, 123.

90 Id. at 121.

91 Id. at 121, 123.

92 Id. (internal quotation marks and original emphasis omitted).

93 Id. at 122 (citing *Skilling v. United States*, 561 U.S. 358, 369 n.1 (2010); *United States v. Garlick*, 240 F.3d 789, 792 (9th Cir. 2001); *United States v. Alston*, 609 F.2d 531, 536 (D.C. Cir. 1979); *United States v. Jefferson*, 674 F.3d 33, 336 (4th Cir. 2012)).

94 Id. at 122–23.

95 Id. at 123.

96 See *United States v. Napout et al.*, 18-2750-cr, 18-2820-cr (CON) (2d. Cir. argued 7 November 2019).

97 See *United States v. Driver*, 692 F. App'x 448, 449 (9th Cir. 2017) ('The focus of the mail and wire fraud statutes is upon the misuse of the instrumentality of communication.' (internal alterations

Circuit observed in *Bascuñán*) other courts, including the Supreme Court, have concluded outside the extraterritoriality context that the focus of the wire fraud statute is the use of domestic wires in furtherance of a scheme to defraud.[98]

29.6 Commodity Exchange Act

The Commodity Exchange Act (CEA), enforced by the Commodity Futures Trading Commission (CFTC), regulates markets in commodities. This broad category embraces 'all services, rights and interests . . . in which contracts for future delivery are presently or in the future dealt in', covering not only traditional commodities like agricultural products,[99] but 'currency and other financial instruments'.[100]

The CEA is aimed at protecting the 'individual investor – who may know little about the intricacies and complexities of the commodities market – from being deceived or misled'.[101] To that end, the statute contains several antifraud provisions.[102] Section 22(a) of the CEA 'establishes a private right of action for individual litigants in four, limited circumstances';[103] in addition, the CFTC may pursue violations through enforcement actions, and the DOJ may bring criminal charges for certain violations.

'Prior to *Morrison*, courts deciding commodities cases applied the same conduct or effects test as was used in the securities context.'[104] But *Morrison* prompted courts to revisit those precedents. In *Loginovskaya v. Batratchenko*,[105] the Second Circuit held that the CEA's private right of action provision, Section 22, 'is silent as to extraterritorial reach' and therefore lacks extraterritorial application.[106] The court then considered the provision's domestic reach. It concluded that the focus of Section 22 is on transactions in commodities, just as the focus of Section 10(b) was found in *Morrison* to be transactions in securities. Accordingly, the court concluded, private suits under the CEA 'must be based on transactions occurring in the territory of the United States'.[107] The court further held that in determining whether a given transaction is domestic, the irrevocable liability test developed

omitted)); *United States v. Coffman*, 574 F. App'x 541, 558 (6th Cir. 2014) ('[W]ire fraud occurs in the United States when defendants use interstate wires as part of their scheme.').

98 See case cited supra note 93.

99 7 U.S.C. § 1a(9).

100 *Salomon Forex Inc. v. Tauber*, 795 F. Supp. 768, 771 (E.D. Va. 1992).

101 *Loginovskaya v. Batratchenko*, 936 F. Supp. 2d 357, 363 (S.D.N.Y. 2013), aff'd, 764 F.3d 266 (2d Cir. 2014).

102 Id.

103 Id. at 364.

104 Id. at 367.

105 764 F.3d 266 (2d Cir. 2014).

106 Id. at 271.

107 Id. at 272. The Second Circuit observed in a later case that the relevant portion of the CEA 'does not contain language similar to the language in § 10(b) that led *Morrison* to craft the "domestic exchange" prong' of its two-pronged test for domestic application (i.e., transactions in securities registered on domestic exchanges, or domestic transactions in other securities). *Myun-Uk Choi v. Tower Research Capital LLC*, 890 F.3d 60, 67 (2d Cir. 2018). The court 'le[ft] aside whether

in the securities context should govern.[108] Therefore, in the Second Circuit, a transaction in a commodity will be regarded as domestic if 'the transfer of title or the point of irrevocable liability . . . occurred in the United States'.[109] Courts applying this standard have stressed the need for plaintiffs to plead and prove facts demonstrating 'the location of the transactions' at issue, including 'the formation of . . . contracts, the placement of orders, the passing of title and the exchange of money'.[110] It is insufficient for the plaintiff to show that he or she is a 'US resident who engaged in . . . futures transactions' from the United States, without proof of 'the location of the transactions themselves'.[111] In addition, the Second Circuit has extended the rule of *Parkcentral*,[112] originally developed in the securities context, to CEA cases. A domestic transaction is therefore necessary but not sufficient for an action under Section 22.[113]

Loginovskaya's statement that Section 22 is 'silent as to extraterritorial reach' is subject to a potential qualification.[114] As the court observed, Dodd-Frank amendments to the CEA altered the statute's reach in a limited set of cases:

> *[Dodd-Frank] amended CEA Section 22 to cover swaps, and provided that its 'provisions . . . relating to swaps' may, under certain circumstances, 'apply to activities outside the United States'.*[115]

Specifically, the CEA provisions regulating swaps apply to activities outside the United States that (1) 'have a direct and significant connection with activities in, or effect on, commerce of the United States', or (2) contravene CFTC rules or regulations aimed at preventing 'the evasion of any provision' added to the CEA

Morrison's discussion of exchanges is applicable to the CEA', concluding that the 'domestic transaction' test was satisfied on the facts before it. Id.

108 See *Loginovskaya*, 764 F.3d at 274; supra Section 29.2.2.

109 Id.

110 *Sullivan v. Barclays PLC*, No. 13-cv-2811-PKC, 2017 WL 685570, at *29 (S.D.N.Y. 21 February 2017).

111 Id.

112 See case cited supra notes 36–39 and related text.

113 See *Prime Int'l*, 2019 WL 4062219, at *6–8. *Prime Int'l* was similar to *Parkcentral* in that the plaintiffs, acting in the United States, traded derivatives pegged to a foreign asset, whose price was allegedly affected by purely foreign conduct (producing losses on the domestic derivatives trades). Id. at *2–3, *8. The court held that plaintiffs were required to show not only a domestic transaction that would satisfy § 22, but domestic conduct that violated a substantive, conduct-regulating provision of the CEA. Id. at *7.

114 764 F.3d at 271.

115 Id. at 271 n.4.

through Dodd-Frank.[116] Because *Loginovskaya* did not involve swaps, the court took 'no view of the effect that the Dodd-Frank amendments may have on the extraterritorial reach of the CEA'.[117]

Some questions of extraterritoriality play out differently in the context of enforcement actions, as opposed to private actions.[118] To begin, several provisions in the CEA expressly grant the CFTC regulatory and enforcement authority over certain conduct involving foreign elements. The statute permits the CFTC to adopt rules proscribing fraud concerning transactions or instruments made on or subject to the rules of foreign exchanges or markets, so long as the regulated behavior is committed by 'any person located in the United States'; it also grants the Commission authority to enforce those rules through lawsuits.[119]

In addition, because enforcement actions do not rely on the transaction-focused private right of action in Section 22, it is likely that some such actions will be permitted to proceed as domestic applications of the CEA based on territorial connections other than US transactions. For example, the Second Circuit has held that the anti-fraud provisions Sections 6(c)(1)[120] and 9(a)(2)[121] centre on manipulation of commodities markets and prices, not on transactions.[122] Similarly, Section 4o, another anti-fraud provision, prohibits commodity trading advisors, and associated individuals or entities, from defrauding clients – without any requirement that the fraud occur in connection with a transaction in a commodity.[123] Given that the provision is not transaction-based, there appears to be no warrant for applying *Morrison*'s 'domestic transaction' test in this context.[124]

---

116 7 U.S.C. § 2(i). Dodd-Frank's limited revision of the extraterritorial reach of the CEA stands in contrast to its (attempted) wholesale revision of the extraterritorial reach of the Exchange Act: While § 929P of Dodd-Frank appears aimed at restoring the conduct-and-effects test in all SEC and criminal actions under the anti-fraud provisions of the Exchange Act, see supra Section 29.2.2, no such sweeping provision was made for CEA cases.

117 764 F.3d at 271 n.4. The Second Circuit again declined to consider the effect of Dodd-Frank's swaps provisions in *Prime Int'l Trading, Ltd. v. BP P.L.C.*, --- F.3d ----, 2019 WL 4062219 (2d Cir. 29 August 2019), concluding that the plaintiffs had forfeited the argument that the CEA applied extraterritorially on that basis. See id. at *5.

118 See id. ('[T]he CEA draws a distinction between the extraterritoriality limits on a private action and enforcement actions brought by the CFTC itself.'); *CFTC v. Vision Fin. Partners, LLC*, 19 F. Supp. 3d 1126, 1131 (S.D. Fla. 2016) (distinguishing, for purposes of extraterritoriality, between private actions and 'suits brought by the Commission itself').

119 *Vision Fin. Partners, LLC*, 190 F. Supp. 3d at *1131 (quoting 7 U.S.C. § 6(b)(2)).

120 'It shall be unlawful for any person, directly or indirectly, to use or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance . . . .' 7 U.S.C. § 9(a)(1).

121 'It shall be a felony . . . for . . . [a]ny person to manipulate or attempt to manipulate the price of any commodity in interstate commerce . . . .' 7 U.S.C. § 13(a)(2).

122 *Prime Int'l*, 2019 WL 4062219, at *8–9.

123 *Loginovskaya*, 936 F. Supp. 2d at 368.

124 Id. at 369 ('*Morrison*'s transaction test is not immediately applicable to § 4o.').

Antitrust 29.7

On its face, the Sherman Act proscribes 'every contract, combination . . . or conspiracy in restraint of trade', but the Supreme Court has held that the Act 'outlaw[s] only *unreasonable* restraints'.[125] Most trade practices are evaluated under the rule of reason, which requires a determination whether, in all the circumstances, 'a restrictive practice should be prohibited as imposing an unreasonable restraint on competition.'[126] But horizontal cartel activity – outright collusion among competitors – is a *per se* violation of the Sherman Act.[127] The antitrust laws are enforced both civilly and criminally, with criminal enforcement generally limited to *per se* violations.[128]

In *Hartford Fire Insurance Co v. California*, decided in 1993, the Supreme Court declared it 'well established by now that the Sherman Act applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States'.[129] That formulation tracked the 'effects' test that *Morrison* would reject in 2010.[130] Arguably, then, *Morrison* may be read to have called into question the continued vitality of *Hartford Fire*.[131]

But *Morrison* has not prompted broad reconsideration of the extraterritorial reach of the Sherman Act, likely for two reasons. First, it may be possible to harmonise *Morrison* and *Hartford Fire*. In *Morrison*, it was held that lower courts had been wrong not to apply the presumption against extraterritoriality in cases where the effects test was satisfied, and should in the future apply the presumption in all cases.[132] One reading of *Hartford Fire* is that the presumption against extraterritoriality is rebutted in Sherman Act cases; that is, the Court's 'effects' language was offered not as a reason to avoid applying the presumption (which would contravene *Morrison*), but as a description of the extraterritorial reach of a statute that overcomes the presumption. Although the majority did not say as much (or mention the presumption at all), the author of the judgment, Justice Scalia, took that view in dissent: 'We have . . . found the presumption to be overcome with respect to our antitrust laws.'[133]

125 *Leegin Creative Leather Prods., Inc. v. PSKS, Inc.*, 551 U.S. 877, 885 (2007) quoting 15 U.S.C. § 1) (emphasis added).

126 Id. (internal quotation marks omitted).

127 Id. at 893.

128 See D. Daniel Sokol, *Reinvigorating Criminal Antitrust?*, 60 Wm. & Mary L. Rev. 1545, 1572–73 (2019).

129 509 U.S. 764, 795–96 (1993).

130 See *Schoenbaum v. Firstbrook*, 405 F.2d 200, 208 (2d Cir. 1968) (citing *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 443–44 (2d Cir. 1945)).

131 See Julie Rose O'Sullivan, *The Extraterritorial Application of Federal Criminal Statutes: Analytical Roadmap, Normative Conclusion, and a Plea to Congress for Direction*, 106 Geo. L.J. 1021, 1049–52 (2018) (noting apparent tension between the Court's antitrust cases and *Morrison*).

132 See *Morrison*, 561 U.S. at 256–61.

133 *Hartford Fire*, 509 U.S. at 813.

Second, when Congress adopted the Foreign Trade Antitrust Improvements Act (FTAIA), it 'expressly endorsed an extraterritorial application of the Sherman Act'.[134] The FTAIA first provides that all foreign commercial activity (except import commerce, namely commerce between foreign sellers and domestic buyers) is 'outside the Sherman Act's reach', but then 'brings such conduct back within' the Act if:[135]

> *(1) the foreign conduct has a 'direct, substantial, and reasonably foreseeable effect' on US domestic, import or certain export commerce; and (2) that effect 'gives rise to a claim under' the Sherman Act.*[136]

This standard is similar (but not identical) to *Hartford Fire*'s rule.[137] Therefore, in antitrust cases involving foreign conduct, there are two related but conceptually distinct paths to extraterritorial application. Foreign activity not subject to the FTAIA (i.e., import commerce) is tested under *Hartford Fire*.[138] Other foreign activity is tested under the similar formulation set out in the FTAIA.[139]

It is therefore clear that the Sherman Act may reach extraterritorial conduct based on domestic effects. For example, in civil cases arising from the manipulation of benchmark interest rates by non-US traders working for defendant banks, courts applied the FTAIA to conclude that conduct occurring abroad was reachable where it affected the price of financial products sold domestically: '[M]

134 *Sonterra Cap. Master Fund v. Credit Suisse Grp.*, 277 F. Supp. 3d 521, 569 (S.D.N.Y. 2017) (internal quotation marks omitted). The FTAIA provides an independent basis for extraterritorial application of the antitrust laws – separate from *Hartford Fire* – because *Hartford Fire* expressly disclaimed any reliance on the FTAIA. 509 U.S. at 796 n.23.

135 *F. Hoffman-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 162 (2004).

136 *Lotes Co., Ltd. v. Hon Hai Precision Indus. Co.*, 753 F.3d 395, 413–14 (2d Cir. 2014) (citations omitted) (quoting 15 U.S.C. § 6a).

137 In addition to requiring that the effect on commerce be 'direct', see *United States v. LSL Biotechnologies*, 379 F.3d 672, 679–80 (9th Cir. 2004), the FTAIA eliminated the requirement that the foreign actor intend to affect US commerce – a product of Congress's determination that a subjective intent-based standard was undesirable and should be replaced with a 'single, objective test'. H.R. Rep. No. 97-686, at 2–3, 9 (1982); see *United States v. Hui Hsiung*, 778 F.3d 738, 748 (9th Cir. 2015) ('[T]he FTAIA's requirement that the defendants' conduct had a 'direct, substantial, and reasonably foreseeable' effect on domestic commerce displaced the intentionality requirement of *Hartford Fire* where the FTAIA applies.').

138 See *Minn-Chem, Inc. v. Agrium, Inc.*, 683 F.3d 845, 855 (7th Cir. 2012) ('[T]he Sherman Act covers imports when actual and intended effects on US commerce have been shown. In *Hartford Fire*, the Supreme Court confirmed this rule, stating that "the Sherman Act covers foreign conduct producing a substantial intended effect in the United States."' (quoting *Hartford Fire*, 509 U.S. at 797)). Of course, for entities that direct goods into domestic commerce through importing activity, the requisite effects will generally be easily proved.

139 Id. at 855–56.

anipulation of a benchmark that is globally disseminated and serves as a pricing component of derivatives sold widely in the United States . . . would have a foreseeable effect within the United States.'[140]

The case law is less clear about what domestic effects count. The Ninth Circuit has interpreted 'direct' in the first prong of the FTAIA – 'direct, substantial, and reasonably foreseeable effect' – to require that the domestic effect follow 'as an immediate consequence of the defendant's activity'.[141] Other courts, including the Second and Seventh Circuits, have embraced what appears to be a weaker conception of directness, expressly rejecting the Ninth Circuit's position and holding that 'the term "direct" means only a reasonably proximate causal nexus.'[142] Despite this overt disagreement, however, there may be little daylight between the competing approaches. The Ninth Circuit has upheld convictions arising from a foreign price-fixing conspiracy where the conspirators fixed the prices of components that were sold abroad and then incorporated into products sold domestically, reasoning that 'the practical upshot of the conspiracy would be and was increased prices to customers in the United States.'[143] In so doing, the court approvingly quoted Seventh Circuit case law contrasting sufficiently direct effects with 'action in a foreign country [that] filters through many layers and finally causes a few ripples in the United States'.[144] In practice – although the precise contours of the rule are unclear – it appears that any of these courts would apply the FTAIA to some foreign anticompetitive conduct that is a step removed from any domestic effects.[145]

Finally, some territorial constraints on private antitrust actions may not apply, or apply differently, in enforcement or criminal actions. For example, in *Motorola Mobility LLC v. AU Optronics Corp*,[146] the Seventh Circuit held that the plaintiff's private action failed under the FTAIA requirement that domestic effects on commerce 'give rise to' the claim, as well as the indirect-purchaser doctrine.[147] But the court cautioned that '[i]f price fixing by the component manufacturers had

140 *Sonterra*, 277 F. Supp. 3d at 569; *Sullivan v. Barclays PLC*, No. 13-cv-2811-PKC, 2017 WL 685570, at *22 (S.D.N.Y. 21 February 2017) ('Defendants also point to the Europe-based conduct of defendants, even though the FTAIA's express language and the decisions applying it focus on the anti-competitive effects within the United States.').

141 *LSL Biotechnologies*, 379 F.3d at 680.

142 *Lotes Co.*, 753 F.3d at 410 (internal quotation marks omitted); see *Minn-Chem*, 683 F.3d at 856–57 (rejecting the Ninth Circuit's test in favour of the 'reasonably proximate causal nexus' formulation).

143 *Hsiung*, 778 F.3d at 759.

144 Id. (quoting *Minn-Chem*, 683 F.3d at 860).

145 Underscoring the lack of practical difference between the two standards, the defendants in *Hsiung* filed a petition for certiorari arguing that the Ninth Circuit's conception of directness was weaker than the Seventh Circuit's. See Pet. for Certiorari 15–16, *Hsiung v. United States*, No. 14-1121 (16 March 2015), cert. denied, 135 S. Ct. 2837 (15 June 2015).

146 775 F.3d 816 (7th Cir. 2015).

147 Id. at 819–23.

the requisite statutory effect on cell phone prices in the United States, the Act would not block the Department of Justice from seeking criminal or injunctive remedies.'[148]

29.8 Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act regulates certain persons and entities by proscribing bribery of foreign officials. The FCPA also prohibits issuers of US securities from falsifying its books and records.[149] As its name suggests, the FCPA applies extraterritorially.[150] But even 'when a statute provides for some extraterritorial application, the presumption against extraterritoriality operates to limit that provision to its terms.'[151] The FCPA sets out with 'surgical precision' the circumstances in which its anti-bribery provisions apply.[152] Specifically, these provisions reach (1) issuers of securities registered on US exchanges or that file periodic reports with the SEC that use interstate commerce in furtherance of a bribery scheme (issuers), (2) United States companies or persons that use interstate commerce in furtherance of a bribery scheme (domestic concerns) and (3) 'foreign persons or businesses taking acts to further certain corrupt schemes, including ones causing the payment of bribes, while present in the United States'.[153] In addition, the statute reaches 'any officer, director, employee, or agent' acting on behalf of a covered entity.[154]

In published guidance and enforcement actions, the government has taken a broad view of the kind of conduct that will render a largely foreign scheme subject to US jurisdiction. Jointly published guidance from the SEC and DOJ states that the use-of-commerce requirement would be satisfied by any telephone call, email, text message or fax to the United States, or by 'sending a wire transfer . . . to a US bank or otherwise using the US banking system'.[155] The government has asserted this view in enforcement actions. For example, in *United States v. JGC Corp*, a Japanese defendant was charged with FCPA violations arising from a scheme to bribe Nigerian officials. The jurisdictional theory was that 'certain alleged bribe payments . . . flowed through US bank accounts and that co-conspirators

148 Id. at 825. Indeed, the same cartel activity was successfully prosecuted in *Hsiung*. See also *Empagran*, 542 U.S. at 170–71 (concluding that plaintiffs' private action failed under the 'give rise to' requirement because their injury flowed purely from foreign effects, and distinguishing earlier cases permitting the government to seek 'relief that might have helped to protect those injured abroad' on the ground that the government enjoys 'broad' authority to 'seek to obtain the relief necessary to protect the public from further anticompetitive harm').

149 15 U.S.C. §§ 78dd-1–3, 78m.

150 See *United States v. Hoskins*, 902 F.3d 69, 96 (2d Cir. 2018).

151 *Morrison*, 561 U.S. at 265.

152 *Hoskins*, 902 F.3d at 84.

153 Id. at 71; see 15 U.S.C. § 78dd-1–3.

154 Id. An agent of a foreign person or business is covered only for acts that occur 'while in the territory of the United States'. 15 U.S.C. § 78dd-3.

155 Criminal Division of the US Department of Justice and Enforcement Division of the US Securities and Exchange Commission, A Resource Guide to the US Foreign Corrupt Practices Act (2012) (FCPA Resource Guide), at 11.

faxed or e-mailed information into the United States in furtherance of the bribery scheme.'[156] The case was resolved through a deferred prosecution agreement (DPA) so the issue was not litigated.[157]

FCPA actions are frequently resolved without adversarial litigation, through plea agreements, DPAs, non-prosecution agreements (NPAs), or SEC 'neither admit nor deny' settlements, so aggressive theories of jurisdiction have rarely been subjected to judicial scrutiny.[158] When they have been, results have been mixed. In *United States v. Patel*, the defendant was not an issuer or a domestic concern (or acting on behalf of such an entity), meaning that he was subject to the FCPA only for acts taken 'while in the territory of the United States'.[159] The government charged an FCPA count based on the defendant's mailing a DHL package from London to the United States.[160] The government acknowledged the requirement of territorial conduct, but argued that this element was satisfied based on separate conduct that formed the basis for a different count; that is, the government theorised that once any domestic conduct was proved, further FCPA counts could be charged based on purely foreign acts.[161] The court disagreed, reasoning that each charged violation had to have occurred while in US territory.[162] In *SEC v. Straub*,[163] the defendants were officers of an issuer – making the requirement of territorial conduct inapplicable – but the government still had to prove that they had used interstate commerce to further their bribery scheme.[164] The government alleged that the defendants had sent e-mails that were 'routed through and/or stored' on US servers.[165] The defendants argued that this element contained a *mens rea* requirement, so that conviction was improper without proof that they knew the emails would be routed through or stored in the United States.[166] The court, addressing 'a matter of first impression in the FCPA context', sided with the government, concluding that the defendants were subject to the FCPA even if they lacked knowledge that their conduct involved interstate commerce.[167]

In addition to pressing aggressive interpretations of the FCPA's textual coverage, the government has also sought to expand the statute's reach through conspiracy and complicity theories. Two recent decisions diverge on whether the government may so employ principles of secondary liability to reach individuals

156 Mike Koehler, The Foreign Corrupt Practices Act in a New Era 110 (2014); see Information 10–17, *United States v. JGC Corp.*, No. 11-cr-260 (S.D. Tex. 6 April 2011).

157 See Deferred Prosecution Agreement, *United States v. JGC Corp.*, No. 11-cr-260 (S.D. Tex. 6 April 2011).

158 See Koehler, supra note 156, at 60–63.

159 15 U.S.C. § 78dd-3(a).

160 Tr. 7–10, *United States v. Patel*, No. 09-cr-335 (D.D.C. 12 August 2011), ECF No. 434.

161 Id.

162 Id. at 11, 29.

163 921 F. Supp. 2d 244 (S.D.N.Y. 2013).

164 Id. at 260, 262.

165 Id. at 262.

166 Id.

167 Id. at 263–64.

who would not otherwise be subject to the FCPA. In *United States v. Hoskins*,[168] prosecutors argued that the defendant, a foreign national employed by a French company who never entered the United States during the alleged scheme, was criminally liable for conspiring with and aiding and abetting employees of his company's US subsidiary in a scheme to bribe Indonesian officials.[169] The Second Circuit rejected that view. The court reasoned that the statute's text and legislative history evinced an affirmative legislative policy to limit liability to the categories of individuals and entities described therein; the government could not override that choice by charging individuals outside those categories under conspiracy or complicity theories.[170] In any event, wrote the court, the presumption against extraterritoriality limits the FCPA's extraterritoriality provisions to their terms, and '[t]he government may not expand the extraterritorial reach of the FCPA by recourse to the conspiracy and complicity statutes.'[171] But a judge in the Northern District of Illinois expressly broke with *Hoskins* in *United States v. Firtash*,[172] concluding that Seventh Circuit precedent on conspiracy and accomplice liability commanded the opposite result.[173] The court permitted the government to proceed against two defendants, neither of whom belonged to 'the class of individuals capable of committing a substantive FCPA violation', on theories of secondary liability.[174] At trial, the district court instructed the jury that an agency relationship requires the following: 'one, a manifestation by the principal that the agent will act for it; two, acceptance by the agent of the undertaking; and, three, an understanding between the agent and the principal that the principal will be in control of the undertaking'. [175] The jury convicted.[176]

Even if *Hoskins* gains wide acceptance among federal courts, the SEC and DOJ are not without tools to reach overseas conduct by foreign nationals. The statute reaches not only issuers and domestic concerns, but their officers, directors, employees and agents.[177] Therefore, in *Hoskins*, the Second Circuit sustained the indictment to the extent it was based on the theory that the defendant acted as an agent of a domestic concern (i.e., the defendant's company's US subsidiary).[178]

The statute does not by its terms extend to foreign subsidiaries of US issuers or domestic concerns. But the government's published guidance states its position that US parents may be held liable for the conduct of their foreign subsidiaries 'under traditional agency principles'.[179] If the government determines that there

168 902 F.3d 69 (2d Cir. 2018).
169 Id. at 72–76.
170 Id. at 76–95.
171 Id. at 95–97.
172 392 F. Supp. 3d 872 (N.D. Ill. 2019).
173 Id. at *11–13.
174 Id. at *11; see id. at *11–13.
175 Trial Tr. 1246–47, *United States v. Hoskins* (D. Conn. 6 November 2019).
176 Jury Verdict, *United States v. Hoskins* (D. Conn. 8 November 2019), ECF No. 583.
177 15 U.S.C. §§ 78dd-1–2.
178 See *Hoskins*, 902 F.3d at 98.
179 FCPA Resource Guide, supra note 155, at 27.

exists an agency relationship between the parent and its subsidiary – based on such factors as 'the parent's control – including the parent's knowledge and direction of the subsidiary's actions, both generally and in the context of the specific transaction', it will view the parent as 'liable for bribery committed by the subsidiary's employees'.[180]

Sanctions 29.9

Starting in earnest in the aftermath of World War I, the United States has pursued its foreign policy goals through imposition of economic sanctions, namely 'the deliberate withdrawal of normal economic relations between [the US] and a target country, government, entity, or individual in order to coerce the target to modify its behavior in a manner consistent with' US policy goals.[181] The statutory basis for most modern sanctions programmes is the International Emergency Economic Powers Act of 1977,[182] which grants the executive broad economic regulatory authority to respond to threats against 'the national security, foreign policy, or economy of the United States'.[183] US sanctions are administered by the Treasury Department's Office of Foreign Assets Control (OFAC), which may impose civil penalties for non-compliance.[184] In addition, the DOJ may seek criminal penalties for wilful violations, including imprisonment and fines up to US$1 million.[185]

See Chapter 26 on fines, disgorgement, etc.

Sanctions programmes 'vary greatly in scope and objective'.[186] OFAC's 'country-based' programmes are aimed at governments, and its 'list-based programmes' are targeted at specific persons.[187] Under list-based programmes, designated entities and individuals are added to OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), which is regularly updated and

180 Id.

181 Court E. Golumbic & Robert S. Ruff III, *Leveraging the Three Core Competencies: How OFAC Licensing Optimizes Holistic Sanctions*, 38 N.C. J. Int'l L. & Com. Reg. 729, 731 (2013).

182 Pub. L. No. 95-223, 91 Stat. 1625 (1997), codified as amended at 50 U.S.C. §§ 1701–1707.

183 50 U.S.C. §§ 1701–1702.

184 Id. § 1705(b).

185 Id. § 1705(a), (c).

186 Golumbic & Ruff III, supra note 181, at 732; see id. at 770 (describing the operation of various programs, from the Cuba program's 'near total embargo on all goods and services' to programmes that 'are not tied to a geographic region, but instead target persons deemed to be engaged in' certain illicit activities).

187 Perry S. Bechky, *Sanctions and the Blurred Boundaries of Int'l Economic Law*, 83 Mo. L. Rev. 1, 4 (2018).

publicly accessible.[188] Once added to the list, '[t]heir assets are blocked and US persons are generally prohibited from dealing with them'[189] unless authorised by OFAC through a licence.[190]

The territorial reach of a given sanctions programme turns on the particular regulations that define its scope. Many prohibitions apply by their terms only to 'US persons',[191] a term that includes 'any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States'.[192] Such prohibitions therefore apply on the basis of both nationality (including the foreign branches of domestic entities) and territoriality (as to foreign nationals). They are broad enough to reach any transactions made using the US financial system – even transactions beginning and terminating abroad that simply pass through domestic correspondent banks (as US dollar-denominated transactions generally do).[193] Moreover, sanctions applicable to Iran and Cuba apply even more broadly, reaching all persons 'subject to the jurisdiction of the United States' – a category embracing (in addition to US citizens or residents, persons in the United States, and US entities) any organisation owned or controlled by a US citizen, resident or entity.[194]

Secondary sanctions, a feature of several US sanctions programmes, are a cousin to extraterritorial primary sanctions.[195] Like primary sanctions (i.e., compliance obligations, the violation of which is civilly or criminally punishable) that

188 See OFAC, Specially Designated Nationals and Blocked Persons List (4 September 2019), available at treasury.gov/ofac/downloads/sdnlist.pdf (last visited 4 September 2019). OFAC also maintains several non-SDN sanctions lists – collected in the Consolidated Sanctions List – including the Foreign Sanctions Evaders List and the Sectoral Sanctions Identifications List. See OFAC, List of Foreign Sanctions Evaders Sanctioned Pursuant to Executive Order 13608 (7 February 2019), available at https://www.treasury.gov/ofac/downloads/fse/fselist.pdf (last visited 12 November 2019) (including entities and individuals determined to have 'engag[ed] in conduct relating to the evasion of US economic and financial sanctions with respect to Iran or Syria'); OFAC, Sectoral Sanctions Identifications List (15 August 2018), available at https://www.treasury.gov/ofac/downloads/ssi/ssilist.pdf (last visited 12 November 2019) (including 'persons determined by OFAC to be operating in' certain sectors of the Russian economy identified by the Secretary of the Treasury).

189 OFAC, Specially Designated Nationals and Blocked Persons List (SDN), available at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx (last visited 12 November 2019).

190 See Golumbic & Ruff III, supra note 181, at 778 ('OFAC issues two types of licenses: (1) general licenses, which are made public and provide universal exemptions to a given set of sanctions, and (2) specific licenses, which are granted only upon application and authorize only the applicant to engage in a specific transaction or category of transaction.' (footnotes omitted)).

191 See, e.g., 31 C.F.R. § 542.206 (prohibiting new investment in Syria by a United States person).

192 See, e.g., 31 C.F.R. § 542.319 (defining the term for purposes of Syrian sanctions).

193 See *United States v. $1,071,251.44 of Funds Associated with Mingzheng Int'l Trading Ltd.*, 324 F. Supp. 3d 38, 43, 52 (D.D.C. 2018); *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 95 (D.D.C. 2017), reconsideration granted in part on other grounds sub nom. *United States v. All Assets Held at Bank Julius, Baer & Co., Ltd.*, 315 F. Supp. 3d 90 (D.D.C. 2018).

194 See 31 C.F.R. § 515.329 (Cuba); id. § 535.329 (Iran).

195 Bechky, supra note 187, at 9.

apply extraterritorially, secondary sanctions apply to conduct occurring outside the United States.[196] But unlike primary sanctions, secondary sanctions are not enforced by fines or imprisonment. Instead, secondary sanctions threaten economic restrictions on a third-party country or its citizens for certain conduct, generally transacting with a target of primary sanctions.[197] For example, the Iran Sanctions Act, enacted in 1996 and amended several times since, 'mandated the imposition of specified sanctions against foreign firms that reached threshold levels of involvement with Iran's energy sector'.[198] Such secondary sanctions are not extraterritorial in the sense of extending US regulatory jurisdiction to foreign conduct – they are not backed by coercive measures like fines or imprisonment – but they can carry significant consequences for violators, and have at times been 'condemned as "extraterritorially" illegal' by US trading partners.[199]

Money laundering 29.10

The Money Laundering Control Act (MLCA) prohibits (among other conduct) engaging in a financial transaction involving the proceeds of 'specified unlawful activity', or transporting money into or from the United States, with intent to promote or conceal specified unlawful activity.[200] The term 'specified unlawful activity' embraces more than 250 predicate offences.[201] The government need only prove that the defendant intended to promote or conceal the specified unlawful conduct, not that he or she actually committed the predicate offence (or even had the capacity to do so).[202]

Section 1956 provides that:

> *There is extraterritorial jurisdiction over the conduct prohibited by this section if: (1) the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States; and (2) the transaction or series of related transactions involves funds or monetary instruments of a value exceeding $10,000.*[203]

This express provision overcomes the presumption against extraterritoriality.

196 See id.

197 See Jeffrey A. Meyer, *Second Thoughts on Secondary Sanctions*, 30 U. Pa. J. Int'l L. 905, 926 (2009).

198 See *United States v. Amirnazmi*, 645 F.3d 564, 579 (3d Cir. 2011) (citing Iran Sanctions Act, Pub. L. No. 104-72, 110 Stat. 1541 (1996) (codified in part at 50 U.S.C. § 1701 (note))).

199 Meyer, supra note 197, at 929.

200 18 U.S.C. § 1956(a)(1), (2).

201 *United States v. Santos*, 553 U.S. 507, 516 (2008).

202 *United States v. Kozeny*, 493 F. Supp. 2d 693, 706 (S.D.N.Y. 2007), aff'd, 541 F.3d 166 (2d Cir. 2008) ("The elements of a money laundering offense do not include, or even implicate, the capacity to commit the underlying unlawful activity.').

203 18 U.S.C. § 1956(f).

A number of courts have addressed the requirement (applicable only in cases in which the defendant is not a US citizen) that 'the conduct occurs in part in the United States.'[204] This requirement does not mean that the defendant must have been physically present in the United States.[205] Courts have held that, irrespective of the defendant's physical presence, 'a transfer from a foreign account to an account in a US financial institution and a transfer from a US account to a foreign financial institution occur in part in the United States under 18 USC Section 1956(f).'[206] Fewer cases have addressed whether Section 1956(f) is satisfied by a transfer from one foreign bank to another that passes through a correspondent or intermediate bank in the United States.[207] On this issue, results have been mixed.[208]

Because the MLCA applies extraterritorially and does not require proof that the defendant engaged (or had the capacity to engage) in specified unlawful activity, prosecutors may use the statute to charge individuals otherwise beyond the reach of US criminal law. For example, foreign officials who take bribes are not subject to FCPA liability. But foreign officials have been prosecuted under the money laundering statute for engaging in transactions to promote or conceal FCPA violations they are incapable of committing.[209]

204 18 U.S.C. § 1956(f)(1).

205 *United States v. Stein*, No. 93-cr-375, 1994 WL 285020, at *4–5 (E.D. La. 23 June 1994).

206 *United States v. Firtash*, 392 F. Supp. 3d 872 (N.D. Ill. 2019), No. 13-cr-515, 2019 WL 2568569, at *9; see *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d 82, 93 (D.D.C. 2017), reconsideration granted in part on other grounds sub nom. *United States v. All Assets Held at Bank Julius, Baer & Co., Ltd.*, 315 F. Supp. 3d 90 (D.D.C. 23 April 2018) (collecting cases).

207 See *United States v. All Assets Held at Bank Julius*, 251 F. Supp. 3d at 95 (characterising the issue as 'a question of first impression in this Court' that 'has not been considered widely').

208 *Compare* id. at 93–96 ('In this case, the United States alleges that *Lazarenko* and his associates transferred millions of dollars to and from accounts and between foreign bank accounts as [electronic funds transfers] that passed through US financial institutions. In the Court's view, this conduct is precisely what Congress intended to prevent in enacting the money laundering statutes – the use of US financial institutions as clearinghouses for criminal money laundering.'), and *United States v. Prevezon Holdings, Ltd.*, 251 F. Supp. 3d 684, 694 (S.D.N.Y. 10 May 2017) ('[T]he use of US correspondent banks to launder illegal proceeds qualifies as domestic conduct.'), with *United States v. Lloyds TSB Bank PLC*, 639 F. Supp. 2d 314, 324 n.4 (S.D.N.Y. 2009) (characterising a correspondent bank transfer as 'peripheral and transitory contact with the United States' that does not satisfy § 1956(f)); see also *Firtash*, 2019 WL 2568569, at *9 (avoiding the question).

209 See, e.g., *United States v. Duperval*, 777 F.3d 1324, 1328–31 (11th Cir. 2015) (former Haitian official found guilty of laundering the proceeds of 'schemes in which international companies gave him bribes in exchange for favors'); Plea Agreement 11–12, *United States v. Mikerin*, No. 14-cr-529-TDC (D. Md. 31 August 2015) (former Russian official pleaded guilty to laundering proceeds of a bribery scheme).

Power to obtain evidence located overseas 29.11

Demands by US prosecutors and regulators for individuals and entities to produce evidence located abroad can lead to conflicts with foreign law. As the DOJ has recognised:

> *Every nation enacts laws to protect its sovereignty and can react adversely to American law enforcement efforts to gather evidence within its borders without authorization. Such efforts can constitute a violation of that nation's sovereignty or criminal law.*[210]

To mitigate against the potential for such conflict, US policy requires prosecutors to attempt to obtain evidence located abroad through mutual legal assistance treaties (MLATs) rather than unilateral compulsory process, such as grand jury and administrative subpoenas. To do otherwise requires prosecutors to obtain written permission from the DOJ's Office of International Affairs.[211] The United States has entered into MLATs with around 70 countries around the world.[212] MLATs enable US prosecutors to deploy foreign law enforcement authorities to gather evidence for US investigations using the power of foreign law to compel production. While MLATs are powerful evidence-gathering tools, the process can be cumbersome and time-consuming, therefore, US law permits prosecutors to obtain orders suspending the running of the limitation period for crimes under investigation for up to three years during the pendency of any MLAT request.[213]

Outside the MLAT process, US prosecutors often utilise *Bank of Nova Scotia* subpoenas to obtain financial records located overseas by serving subpoenas on US branches of foreign financial institutions.[214] These subpoenas have been upheld by US courts even when compliance would require the subpoena recipient to violate foreign law.[215] Such was the case recently in *In Re: Sealed Case*, in which the DC Court of Appeals upheld civil contempt findings against three Chinese banks that had been served with subpoenas to produce records located in China, the production of which they maintained would violate Chinese law.[216] Two of the banks had US branches and were served with grand jury subpoenas. The third bank did not have a US branch and was served pursuant to a Patriot Act subpoena that gives prosecutors 'special investigatory tools when it comes to US correspondent bank accounts'.[217] The DOJ did not attempt to first gather the evidence sought pursu-

210 DOJ, Justice Manual § 9-13.510.

211 DOJ, Justice Manual § 9-13.525

212 The United States has also entered into agreements that do not rise to the treaty level, mutual legal assistance agreements (MLAAs) with China and the American Institute in Taiwan and the Taipei Economic and Cultural Representative Office in the United States.

213 18 U.S.C. § 3292.

214 *In re Grand Jury Proceeding*, 691 F.2d 1384 (11th Cir. 1982).

215 Id.

216 932 F.3d 915 (D.C. Cir. 2019).

217 Id. at 920; 31 U.S.C. § 5318(k)(3)(A).

ant to the mutual legal assistance agreement with China, arguing that any such attempt would be futile.[218] After conducting a comity analysis, the Court agreed and found that US interests outweighed the Chinese interests at issue.[219]

Conclusion

29.12 US authorities continue to investigate and bring cases based on conduct that largely takes place outside the United States. Practitioners should carefully analyse the conduct at issue and the elements of the applicable statutes to determine whether the conduct is outside the reach of US law.

218 932 F.3d at 936.
219 Id.

30

Individual Penalties and Third-Party Rights: The UK Perspective

Elizabeth Robertson[1]

Individuals: criminal liability 30.1

The Serious Fraud Office (SFO) has agreed to a total of five deferred prosecution agreements (DPAs)[2] with corporates since their introduction in February 2014.[3] The introduction of DPAs reflects a long-standing practice in the United States of granting corporates amnesty from prosecution on criminal charges, either through the use of non-prosecution agreements or DPAs, in exchange for the fulfilment of certain requirements. However, it has been argued: 'An increased focus on corporate criminal liability should not result in the culpability of offending individuals within a corporation being overlooked.'[4] Terms of a DPA will likely require the company to co-operate on an ongoing basis, which may include co-operation in the prosecution of individuals. For example, the *Rolls-Royce* DPA requires Rolls-Royce to 'co-operate . . . in any investigation or prosecution of any of its present or former officers, directors, employees'.[5] However, to date, the SFO has not been successful in prosecuting any individual involved in the conduct related to a DPA.

1 Elizabeth Robertson is a partner at Skadden, Arps, Slate, Meagher & Flom (UK) LLP.

2 DPAs are only available to corporate organisations.

3 See *Standard Bank*, available at https://www.sfo.gov.uk/2015/11/30/sfo-agrees-first-uk-DPA-with-standard-bank/; XYZ, available at https://www.sfo.gov.uk/2016/07/08/sfo-secures-second-dpa/; *Tesco*, available at https://www.sfo.gov.uk/2017/04/10/sfo-agrees-deferred-prosecution-agreement-with-tesco/; *Rolls-Royce*, available at https://www.sfo.gov.uk/cases/rolls-royce-plc/, accessed 18 November 2019.

4 V K Rajah SC, Prosecution of financial crimes and its relationship to a culture of compliance, Company Lawyer, 2016, at p. 5, accessed via Westlaw UK.

5 *Rolls-Royce*, available at https://sfo.gov.uk/cases/rolls-royce-plc/ at paras. 10, 11.

On 6 August 2019, the SFO published its Corporate Co-operation Guidance, which forms part of the SFO's Operational Handbook. The guidance seeks to formalise the approach adopted during previous DPAs and outlines what the SFO expects corporates seeking to co-operate to provide in respect of individuals. It states that corporates should consult with the SFO before interviewing potential witnesses or suspects to avoid prejudice to the investigation, identify potential witnesses, make employees (and, where possible, agents) available for SFO interviews (including arranging for them to return to the UK if necessary) and provide the last known contact details of ex-employees, agents and consultants if requested. Corporates seeking co-operation credit by providing witness accounts also need to provide any recordings, notes and transcripts of the interview.

The SFO continues to signal that individual penalties will become increasingly important, and the relatively recent changes in the test for 'dishonesty' in criminal law may have the effect of encouraging prosecutors to pursue individuals for offences involving dishonesty, such as fraud or theft.

Under the test for dishonesty in *R v. Ghosh*,[6] the jury was first asked to consider whether the defendant's acts were dishonest by the ordinary standards of reasonable honest people. If the answer to that question was 'yes', the jury would then consider whether the defendant must have realised that their conduct was dishonest by those standards. In the recent case of *Ivey v. Genting Casinos t/a Crockfords*,[7] the Supreme Court held that the second limb of the *Ghosh* test no longer represents the law and that directions based on it should no longer be given to juries. The defendant's conduct, in light of his or her (subjective) knowledge or belief of the facts, must be judged as honest or dishonest by the (objective) standards of ordinary decent people alone. The defendant's (subjective) appreciation of whether his or her conduct would be dishonest according to those standards is not relevant. This change will make it more difficult for defendants to escape liability on the basis of their own moral compass and potentially easier for prosecutors to secure a conviction.

The fact that 'the most serious cases of bribery generally involve companies'[8] renders the maximum custodial sentences for financial crimes somewhat obsolete as individuals escape the maximum sentences for these serious corruption cases, which instead are borne by corporate entities and their shareholders in the form of unlimited fines. As Richard Alexander comments, 'any kind of agreement that penalises the company concerned, but does not deal with the individuals who were actually behind the commercial bribery, whether by paying the bribes or by arranging for others to do so, fails to recognise the essential nature of what took place.'[9]

6 [1982] QB 1053.

7 [2017] UKSC 67; also confirmed in *R v. Alex Julian Pabon* [2018] EWCA Crim 420.

8 Richard Alexander, The Bribery Act 2010 in force: an opportunity to be taken, Company Lawyer, 2011, at p. 2, accessed via Westlaw UK.

9 Ibid. at p. 2.

Individual penalties are important because they deter offending in the first place. Further, in instances where the individuals alone are punished, it ensures that innocent parties, such as the shareholders, pension funds and other stakeholders in the company, are not punished indirectly; and where the corporate also faces a penalty, the stakeholders can rest assured that the wrongdoing within the company has almost certainly been dealt with.

While DPAs in the United Kingdom are not available for individuals – and there is no indication that they will be any time soon – there is an increasing emphasis on incentivising individuals to enter an early plea. Enshrined in section 144 of the Criminal Justice Act 2003 (CJA 2003) is the statutory authority that compels the courts to consider a reduction in the sentence of an offender who has pleaded guilty to an offence. Subsection 1 obliges the court to take into account the stage in the proceedings that the offender indicated an intention to plead guilty; and the circumstances in which this indication was given. The Reduction in Sentence for a Guilty Plea: Definitive Guideline (Definitive Guideline) guides the courts in establishing an appropriate level of reduction for the offender in question.[10] Unless, on the facts, there is a sufficiently good reason for a lower amount, there is a presumption that for each of the following categories, the recommended reduction will be given. If the offender pleads guilty (1) at the first stage of proceedings, he or she can expect the sentence to be reduced by a maximum of one-third; (2) after the first stage of the proceedings, the offender may receive a maximum of a one-quarter reduction in the sentence; or (3) after the trial has begun, the reduction should be decreased from one-quarter to a maximum of one-tenth. Where the guilty plea is entered during the course of the trial, the reduction should normally be decreased further, even to zero. The Serious Organised Crime and Police Act 2005[11] contains several provisions that can benefit an offender who assists in the investigation or prosecution of a crime. For example, if an offender provides or offers assistance in the investigation or prosecution of others, the court in return may reduce the offender's sentence.[12] A defendant, already serving a prison sentence, who provides or offers assistance in this regard could also benefit by having a sentence reviewed.[13]

Imprisonment 30.1.1

Pursuant to section 11 of the Bribery Act 2010 (Bribery Act), the maximum sentence for an individual convicted on indictment of an offence by virtue of sections 1, 2 or 6 of the Bribery Act is 10 years' imprisonment.[14] Furthermore, under section 14 of the Bribery Act, if a corporate commits an offence under section 1, 2 or 6, if the offence is proved to have been committed with the consent

10 The Definitive Guideline was updated on 1 June 2017.

11 Chapter 2 (ss. 71–75).

12 s.73 Serious Organised Crime and Police Act (SOCPA).

13 s.74 SOCPA.

14 An individual cannot be convicted of an offence under s.7 of the Bribery Act because the offence refers only to a 'commercial organisation' for which the only sentence available is an unlimited fine.

or connivance of a senior officer (or person purporting to act in such a capacity), that officer or person can also be punished. An individual tried and convicted summarily of any of the aforementioned offences is liable to a maximum prison sentence of 12 months. An individual convicted following summary trial will (if the offence merits more severe sanction) be committed to the Crown Court for sentence. The maximum sentence for individuals under the Bribery Act is identical for any of the fraud offences both at common law and under the Fraud Act 2006 but is far greater (up to a maximum of 14 years' imprisonment) for any of the substantive money laundering offences pursuant to sections 327 to 329 of the Proceeds of Crime Act 2002 (POCA). Furthermore, an individual convicted of the tipping- off offence under section 333A of POCA is liable to a maximum of two years' imprisonment or to a fine, or both.

Historically, under the corruption regime that persisted until the later part of the 20th century, individuals were liable to three years' imprisonment on conviction of corruption charges. This was subsequently increased to seven years under the Criminal Justice Act 1988[15] and increased again under the current regime. The shift in policy in relation to the penalties imposed on individuals who commit financial crime can largely be attributed to the distrust and anger felt by the public towards misconduct in big business; particularly following the 2008 financial crisis. Nowhere is this so apparent than in the case of Tom Hayes. Mr Hayes is currently serving an 11-year prison sentence (which was reduced on appeal from an original sentence of 14 years), one of the longest prison terms on record for UK white-collar crime,[16] for his role in the manipulation of the London Interbank Offered Rate while he worked as a derivatives trader at two different investment banks. It is widely accepted that the hefty sentence was handed down to serve as a warning to other individuals who may be tempted by the allure of profit to participate in such practices. In passing sentence, the court said that it 'must make clear to all in the financial and other markets in the City of London that conduct of this type, involving fraudulent manipulation of the markets, will result in severe sentences of considerable length which, depending on the circumstances, may be significantly greater than the present total sentence.'[17] The case was accepted for review by the Criminal Cases Review Commission in June 2017, and an outcome is still pending.

Additionally, on 19 July 2018, Christian Bittar (Deutsche Bank) and Philippe Moryoussef (Barclays Bank) were sentenced to a total of 13 years and 4 months' imprisonment for manipulating the Euro Interbank Offered Rate.[18] In the same trial, the jury was unable to reach verdicts on Carlo Palombo, Colin Bermingham and Sisse Bohart, formerly of Barclays Bank, but the SFO proceeded with a retrial,

15 See s.47 of the Criminal Justice Act 1988.

16 https://www.theguardian.com/business/2015/dec/21/libor-trader-tom-hayes-loses-appeal-but-has-jail-sentence-cut-to-11-years, accessed 18 November 2019.

17 *R v. Hayes* [2015] EWCA Crim 1944, at para. 109.

18 https://www.sfo.gov.uk/2018/07/19/senior-bankers-sentenced-to-more-than-13-years-for-rigging-euribor-rate/, accessed 18 November 2019.

and in March 2019, Mr Palombo and Mr Bermingham were convicted (and Ms Bohart acquitted). In April 2019, Mr Palombo and Mr Bermingham were sentenced to a total of nine years' imprisonment.[19]

In cases of financial crime, it is rare for defendants to be charged with only one count, and in the most serious cases – and as was the case for Mr Hayes – a judge can order the sentences for each individual count of which a defendant has been convicted to run consecutively. According to a Reuters news report: 'Hayes was sentenced consecutively for the conspiracies he was found guilty of while at two investment banks between 2006 and 2010. Had the market rigging been seen as one offence, Hayes would have faced a maximum 10-year sentence.'[20] Whether a judge perceives a concurrent or consecutive sentence as appropriate on the facts will be decided by reference to the same factors that judges tend to consider when deciding on the severity of a sentence, such as whether the defendant has any previous convictions, the magnitude of the offence[21] or where it can be established that the defendant failed to respond to warnings about his or her behaviour. Magnus Peterson was sentenced on eight counts of fraud, forgery, false accounting and fraudulent trading to 13 years in prison on 23 January 2015.[22]

Despite the continued prominence of financial crime cases in the media and the apparent fervour of prosecutors and courts to ensure that convicted individuals receive long custodial sentences, suspended sentences may well be considered appropriate in some cases. In *R v. Dougall*,[23] an employee heading a company's corrupt Greek practice who pleaded guilty to conspiracy to corrupt, and who was a co-operating defendant under section 73 SOCPA, had his 12-month custodial sentence suspended on appeal. The Court of Appeal held that 'where the appropriate sentence for a defendant whose level of criminality,[24] and features of mitigation, combined with a guilty plea, and full co-operation with the authorities investigating a major crime involving fraud or corruption, with all the consequent burdens of complying with his part of the SOCPA agreement, would be 12 months' imprisonment or less, the argument that the sentence should be suspended is very powerful.'[25] This case also demonstrates the risks individuals face when conduct spans multiple jurisdictions and no settlement or amount of

See Chapter 17 on individuals in cross-border proceedings

19 https://www.sfo.gov.uk/2019/04/01/senior-bankers-sentenced-to-9-years-for-rigging-euribor-rate, accessed 18 November 2019.

20 http://www.reuters.com/article/us-libor-hayes-appeal-idUSKBN0TJ1V820151130, 30 November 2015, accessed 18 November 2019.

21 In the Fraud, Bribery and Money Laundering Offences Definitive Guideline, it expressly states that: 'Consecutive sentences for multiple offences may be appropriate where large sums are involved.' https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-Bribery-and-Money-Laundering-offences-definitive-guideline-Web.pdf, at p. 10, accessed 18 November 2019.

22 https://www.sfo.gov.uk/2015/01/23/magnus-peterson-sentenced-13-years-prison/, accessed 18 November 2019.

23 [2010] EWCA Crim 1048.

24 Mr Dougall had failed to convince other employees to end the practice of making corrupt payments to medical professionals to persuade them to buy the company's goods.

25 *R v. Dougall* [2010] EWCA Crim 1048, at para. 36.

See Chapter 23 on negotiating global settlements

co-operation provides an absolute guarantee against further proceedings being pursued in any jurisdiction.

The Attorney General's Guidelines on Plea Discussions in Cases of Serious or Complex Fraud (Attorney General's Guidelines) set out a process by which a prosecutor may discuss an allegation of serious or complex fraud with a suspect.[26] The implementation of the Attorney General's Guidelines, with the support of the judiciary and prosecuting authorities, has garnered a quasi-plea discussion system that can be advantageous to defendants. Although the Attorney General's Guidelines do not make any provision for a defendant to receive a greater discount on the sentence than is available for simply entering a guilty plea (as set out above), in a case brought by the Financial Services Authority (FSA)[27] against Paul Milsom, a senior equities trader, for disclosing inside information between October 2008 and March 2010, Judge Pegden QC indicated, in passing sentence on 18 March 2013 at Southwark Crown Court, that he had given Mr Milsom full credit for pleading guilty at the earliest opportunity (i.e., a discount of one-third) and extra credit for entering into a plea agreement with the FSA.[28] The sentencing remarks of Judge Pegden QC convey the 'clearest articulation to date that an individual can reasonably expect to receive in excess of one third discount on sentence in circumstances where he enters into early plea discussions with a prosecutor.'[29]

In *Bittar*, when sentencing, the judge also took into consideration Mr Bittar's early guilty plea, along with other mitigating factors such as the delay between the period of offending and the resulting trial, the low likelihood of further future offending and Mr Bittar's previous good character.[30]

Another case worthy of note, and one that again highlights how co-operation with the authorities can really pay dividends when it comes to sentencing after conviction, was that of Bruce Hall. On 22 July 2014, Mr Hall, CEO of Aluminium Bahrain BSC from September 2001 to June 2005, received a 16-month custodial sentence[31] for conspiracy to corrupt (having allegedly received £2.9 million in bribes[32]). However, were it not for Mr Hall's co-operation and early plea, Judge Loraine-Smith stated that his prison sentence would have been far longer. According to the SFO website, 'Mr Hall had co-operated with numerous

26 The Attorney General's Guidelines came into force on 5 May 2009.

27 As of 3 April 2013, the FSA became two separate regulatory bodies; the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA).

28 https://webarchive.nationalarchives.gov.uk/20130402175500/http://www.fsa.gov.uk/library/communication/pr/2013/022.shtml, accessed 18 November 2019.

29 Chris Dyke, The Benefits of Early Plea Discussions, https://www.corkerbinning.com/corker-binning-solicitor-writes-about-the-benefits-of-early-plea-discussions-in-crimeline/, accessed 18 November 2019.

30 https://www.sfo.gov.uk/2018/07/19/senior-bankers-sentenced-to-more-than-13-years-for-rigging-euribor-rate/, accessed 18 November 2019.

31 Mr Hall was also ordered to pay a confiscation order of £3,070,106.03 within seven days or face serving an additional term of imprisonment of 10 years; a compensation order of £500,010; and to pay £100,000 as a contribution to the prosecution's costs.

32 https://www.sfo.gov.uk/2014/07/22/bruce-hall-sentenced-16-months-prison/, accessed 18 November 2019.

authorities throughout the investigation. If he had not been so co-operative, Mr Hall could have faced around six years in prison, close to the maximum sentence for conspiracy to corrupt, the judge said. Due to his co-operation, Mr Hall was entitled to a 66 per cent reduction in his sentence. He was also entitled to a further reduction of one-third due to entering a guilty plea.'[33] The case demonstrated that civil recovery proceedings and criminal proceedings are not mutually excluded provided that the conduct can be divided.

See Chapter 23 on negotiating global settlements

Fines 30.1.2

Fines for individual perpetrators of financial crime can be unlimited and are handed down either separately or in conjunction with a custodial sentence. Section 164 of the CJA 2003 regulates the fixing of fines in criminal cases. The Sentencing Council's Fraud, Bribery and Money Laundering Offences Definitive Guideline states that as a general principle in the setting of a fine for fraud, bribery or money laundering: 'The court should determine the appropriate level of fine in accordance with section 164 of the Criminal Justice Act 2003, which requires that the fine must reflect the seriousness of the offence and requires the court to take into account the financial circumstances of the offender.'[34]

Unexplained wealth orders 30.1.3

The Criminal Finances Act 2017 (CFA 2017) came into force on 30 September 2017 and created a new High Court power to make an unexplained wealth order (UWO), which can require a person who is suspected of involvement in, or association with, serious criminality or who is a politically exposed person (PEP) to explain the origin of assets that appear to be disproportionate to their known income.[35] A failure to provide a response will give rise to a presumption that the property is recoverable, in order to assist any subsequent civil recovery action. UWOs are intended to alleviate the burden on enforcement authorities and come with wide-ranging powers to gather evidence in other jurisdictions and potentially support parallel enforcement actions. The powers to make UWOs under the CFA 2017 commenced on 31 January 2018, with the National Crime Agency (NCA) obtaining four UWOs in the first 18 months of commencement.[36]

The CFA 2017 enables a number of UK regulators and enforcement agencies, namely the SFO, the NCA, HM Revenue and Customs, the FCA and the Director of Public Prosecutions, to apply to the High Court for a UWO, regardless of whether civil or criminal proceedings have been initiated against the respondent to the order or whether the respondent is located in the United Kingdom or another jurisdiction.

33 Ibid., accessed 29 July 2016.

34 https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-Bribery-and-Money-Laundering-offences-definitive-guideline-Web.pdf, at p. 51, accessed 18 November 2019.

35 Under Part 1 ss.1-9 of the Criminal Finances Act 2017, which amends POCA s.362.

36 Barney Thompson, 'Mystery banker's wife challenges UK unexplained wealth order', *Financial Times*, accessed 18 November 2019.

There must be reasonable cause to believe that the respondent holds the property and that the value of the property is greater than £50,000. There must also be reasonable grounds for suspecting that the known sources of the respondent's lawfully obtained income would have been insufficient for the purposes of enabling the respondent to obtain the property. Respondents must also either be (1) a PEP or (2) someone for whom there are reasonable grounds for suspecting that they have been involved in serious crime. Under the CFA 2017, a person is considered to be involved in serious crime in the United Kingdom or another jurisdiction if the person would be so involved for the purposes of Part 1 of the Serious Crime Act 2007. This widens the category of potential respondents significantly to include persons who: (1) have committed a serious offence; (2) have facilitated the commission of an offence; or (3) conducted themselves in a way that was likely to facilitate the commission by themselves – or another person – of a serious offence, whether or not the offence was committed. The CFA 2017 widens the category of respondents even further to include anyone who is connected with a person who is or has been involved in serious crime, whether in the United Kingdom or in another jurisdiction.

The first UWO, obtained in February 2018, was made against two properties valued at approximately £22 million, connected to Mrs Zamira Hajiyeva, the wife of Mr Jahangir Hajiyev, a former banker imprisoned for fraud and embezzlement in Azerbaijan. Mrs Hajiyvera challenged the orders in the High Court on a number of grounds, including that her husband had been incorrectly classified as a PEP. However, the court dismissed these challenges, finding that Mr Hajiyev was a PEP from a non-EEA country against whom an UWO could be granted, and that as his wife, Mrs Hajiyvera was herself also a PEP.[37] The second UWO was also made against property belonging to a PEP. In this instance, the three properties subject to the UWO were worth in excess of £80 million, owned by an unnamed foreign official. Only on 12 July 2019 did the NCA obtain its first UWO against a respondent considered to be involved in serious crime.[38] The NCA press release stated, 'Officers believe the businessman's property purchases valued at £10 million were funded by a number of criminal associates involved in drug trafficking, armed robberies and supplying firearms.' A second UWO against a respondent considered to be involved in serious crime followed shortly thereafter on 24 July 2019. On this occasion, the UWO was obtained against six properties worth around £3.2 million in total belonging to a woman believed to be associated with criminals involved in paramilitary activity and cigarette smuggling.[39]

Interim freezing orders can also be granted by the High Court with each UWO, under section 362J POCA, meaning that the assets subject to the UWOs cannot be sold, transferred or dissipated for the duration of the order.

37 *National Crime Agency v. Mrs A* [2018] EWHC 2534 (Admin).

38 https://www.nationalcrimeagency.gov.uk/news/nca-secures-first-serious-organised-crime-unexplained-wealth-order-for-property-worth-10-million, accessed 18 November 2019.

39 https://www.nationalcrimeagency.gov.uk/news/nca-secures-unexplained-wealth-order-against-properties-owned-by-a-northern-irish-woman, accessed 18 November 2019.

Respondents are required by a UWO to provide certain information about the specified property, including the nature and extent of the respondent's interest, how it was obtained and any other information specified in the order. Aside from contempt of court proceedings, the failure to respond to a UWO creates a presumption that the property is recoverable in civil proceedings, which reduces the burden imposed on enforcement authorities under the current POCA regime, to prove that property derives from criminal conduct or constitutes the proceeds of crime. Section 362S of POCA provides that when a UWO is issued, where the enforcement authority believes that the property is outside the United Kingdom, it may send a request for assistance in relation to the property to the Secretary of State, who in turn may forward the request to the government of the receiving country. The request for assistance is a request that any person be prohibited from dealing with the property or assisting with dealing with the property.

Where a respondent complies or purports to comply, the enforcement authority must determine, within 60 days starting with the date of compliance, what enforcement or investigatory proceedings, if any, it considers ought to be taken in relation to the property.

POCA also provides that a criminal offence is committed if a respondent gives a false or misleading statement in response to a UWO, with a maximum penalty of two years' imprisonment.[40] The CFA 2017 amends POCA so that the FCA and HMRC have civil recovery powers to recover property in cases where there has not been a conviction but where it can be shown on the balance of probabilities that property has been obtained by unlawful conduct. Such proceedings would be brought in the High Court to recover criminal property without the need for the owner of the property to be convicted of a criminal offence.

Confiscation orders 30.1.4

It is becoming more common for courts to address the confiscation of the assets of a convicted individual, especially when the court satisfies itself that the defendant was said to be living a 'criminal lifestyle'.[41] Furthermore, Step 6 of the Sentencing Council Guidelines on Fraud, Bribery and Money Laundering Offences states that the court must proceed with a view to making a confiscation order if it is asked to do so by the prosecutor or if the court believes it is appropriate to do so.[42] The FCA secured £1.9 million in confiscation orders on 11 May 2018, as part of

40 s.362E CFA 2017.

41 Pursuant to s.75 of the CJA 2003, '(1) a defendant has a criminal lifestyle if (and only if) the following condition is satisfied. (2) The condition is that the offence (or any of the offences) concerned satisfies any of these tests – (a) it is specified in Schedule 2; (b) it constitutes conduct forming part of a course of criminal activity; or (c) it is an offence committed over a period of at least six months and the defendant has benefited from the conduct which constitutes the offence'.

42 https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-Bribery-and-Money-Laundering-offences-definitive-guideline-Web.pdf, accessed 18 November 2019.

Operation Tabernula, and £2.2 million in confiscation orders in May 2017, as part of Operation Cotton.[43]

Confiscation orders, which are debts to the Crown, are available only after a defendant has been convicted. Where a confiscation order is not paid, the defendant will serve a period of imprisonment in default. This mechanism is highlighted in the cases of (1) Phillip Boakes, who, after failing to satisfy the full value of a confiscation order determined by the courts, was ordered to serve 730 days' imprisonment in addition to the 10 years he was already serving after pleading guilty, *inter alia*, to two counts of fraudulent trading;[44] (2) Alex Hope, who was sentenced to 603 days' imprisonment for failing to pay the full value of a confiscation order made against him, in addition to the seven years he was serving for defrauding investors;[45] and (3) Peter Chapman, who in September 2019 was ordered to pay a confiscation order of £441,944.38 and failure to pay within three months will result in him returning to prison for a default sentence of four years.[46]

The Supreme Court also recently clarified the position regarding the reduction of default sentences for partial repayment of sums ordered under a confiscation order. In *R (on the application of Gibson) v. Secretary of State for Justice*,[47] the Supreme Court held that the calculation of reductions in default terms should not take into consideration accrued interest. The appellant had been convicted of a drug trafficking offence in 1999 and sentenced to 25 years' imprisonment. At a confiscation hearing in 2000, he was ordered to pay £5.4 million within 12 months or serve a six-year default sentence and accrue 8 per cent interest per annum. The appellant did not pay the amount ordered, triggering the accrual of interest on the outstanding amount. By the time the appellant was committed to prison under the default sentence, the outstanding amount was £8.1 million. However, £90,370 had been paid off the order, entitling the appellant to a reduction in his default sentence. The issue for the courts was therefore to determine whether the reduction should be calculated as a percentage of the initial £5.4 million order or of £8.1 million. The appellant argued that the calculation should be based on the original £5.4 million order, entitling him to a reduction of 35 days. However, in the Administrative Court and Court of Appeal it was held that a reduction of only 24 days should be applied, calculated on the basis of the £8.1 million outstanding. In January 2018, the Supreme Court held in the appellant's favour, entitling him to the additional 11-day reduction in his default

43 https://www.fca.org.uk/news/press-releases/fca-secures-confiscation-orders-totalling-1-69-million-against-convicted-insider-dealers; https://www.fca.org.uk/news/press-releases/fca-secures-eight-confiscation-orders-totalling-almost-22-million, accessed 18 November 2018.

44 https://www.fca.org.uk/news/phillip-boakes-sentenced-for-failing-to-pay-confiscation-order, accessed 18 November 2019.

45 https://www.fca.org.uk/news/press-releases/alex-hope-sentenced-failing-pay-confiscation-order, accessed 18 November 2019.

46 https://www.sfo.gov.uk/2019/09/05/currency-fraudster-peter-chapman-ordered-to-pay-441944-38/, accessed 18 November 2019.

47 [2018] UKSC 2.

sentence. The ruling confirms that there is a continued incentive for individuals subject to confiscation orders to continue making contributions even after a default sentence has been triggered.

Confiscation orders derive from section 6 of POCA and are intended to deprive the defendant of the benefit of any proceeds of his or her crimes; they are not, however, intended to act as a fine or further punishment. They do not always involve the sequestration of the defendant's personal property. Instead, they usually entail the payment of a sum of money: 'Where, however, a criminal has benefited financially from crime but no longer possesses the specific fruits of his crime, he will be deprived of assets of equivalent value, if he has them.'[48] In accordance with the decision in *R v. Waya*,[49] prosecutors should ensure that the confiscation is proportionate, which entails an assessment of the ability of the defendant to pay the order in full.

In determining the amount of £165,731 that Mr Boakes was required to pay under his confiscation order, the court was able to take into account how the money that he had acquired was spent. The court determined that much of the proceeds that Mr Boakes had benefited from was spent on a lavish lifestyle and unsuccessful financial trading that was indicative of a criminal lifestyle, which the courts will take into account when determining the recoverable amount.

The Attorney General's Guidelines are silent as to confiscation orders – they provide no framework to regulate the discussions and agreement of confiscation orders as part of plea discussions. Should the prosecution and the defendant reach any form of agreement in relation to a confiscation order, that agreement would not bind a court. In Mr Milsom's case, however, the judge agreed to make a confiscation order at the sentencing hearing in the value of his personal benefit from his offending, which had been agreed between the prosecution and the defence within the basis of the plea and joint sentencing submission. This suggests that prosecutors could be willing to negotiate the terms of a confiscation order as part of a plea negotiation, and that the courts may be willing to accept the joint submission that 'provid[es] a defendant with greater certainty and control over his financial liabilities'.[50]

The burden of proof in criminal confiscation orders rests with the defendant, who must show, on the balance of probabilities, that his or her assets are not derived from criminal conduct.

Where it is reasonably foreseeable that a court will make a confiscation order, the prosecution may take steps in the High Court to ensure that the defendant's assets will remain available to meet the terms of the order. Such steps include, *inter*

48 *R v. May* [2008] UKHL 28, at para. 9.

49 [2012] UKSC 51.

50 Chris Dyke, The Benefits of Early Plea Discussions, https://www.corkerbinning.com/corker-binning-solicitor-writes-about-the-benefits-of-early-plea-discussions-in-crimeline/, accessed 18 November 2019

alia, an order requiring the defendant to disclose where assets are kept, an order appointing a receiver and an order restraining assets.[51]

30.1.5 Compensation orders

Like a confiscation order, a compensation order is an ancillary court order and is designed to compensate a victim for personal injury or any loss or damage that may have resulted from the offence committed by the defendant and is made in addition, or instead of, other sentencing options under section 130 of the Powers of Criminal Courts (Sentencing) Act 2000. The Sentencing Council Guidelines on Fraud, Bribery and Money Laundering Offences also provide that, under Step 6, the court must proceed with a view to making a confiscation order, if it is asked to do so by the prosecutor, or if the court believes it is appropriate to do so.[52]

In both a magistrates' court[53] and the Crown Court, the amount that can be awarded as compensation is now unlimited but is restricted to an amount that can feasibly be paid by the defendant. The court must have regard to the evidence of the defendant's financial means when deciding the level of compensation to award the victim and must prioritise the payment of compensation over any other financial penalty.

30.1.6 Disqualification orders

Directors of companies are fiduciaries and there is consequently a high level of probity expected of them by the law. It is therefore expected that '[t]hose who are involved in bribery, whether as individuals or as part of their role as directors, are very likely to be disqualified from acting as a director for a lengthy period of time.'[54]

See Chapter 25 on fines, disgorgement, etc. and Chapter 41 on directors' duties

Directors disqualification orders (DDOs) are designed to help protect creditors and the public from those individuals who may act dishonestly and can bar a person from acting as a director of any UK company for up to 15 years. DDOs can be made where the defendant director of a company has been convicted of an indictable offence which, by virtue of the decision in *R v. Creggy*,[55] must have some relevant factual connection with the management of the company.

30.1.7 Costs

As in all criminal cases, cost orders are usually made against a convicted defendant, who will be required to pay the prosecution's costs as well as any court fees that materialise during the criminal proceedings.

---

51 See s.37(1) Supreme Court Act 1981.

52 https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-Bribery-and-Money-Laundering-offences-definitive-guideline-Web.pdf, accessed 18 November 2019.

53 Before 11 December 2013, the amount that a magistrate could award as part of a compensation order was £5,000, but, by virtue of s.131 Powers of Criminal Courts Sentencing Act 2000, this limit has been removed.

54 Eoin O'Shea, *The Bribery Act 2010, A Practical Guide*, Jordans, at p. 238.

55 [2008] EWCA Crim 394.

The legislative authority enabling a court to award costs in criminal proceedings is primarily contained in Part II of the Prosecution of Offences Act 1985 (sections 16 to 19B), the Access to Justice Act 1999 (in relation to funded clients) and in regulations that have since been made pursuant to these statutes, including the Costs in Criminal Cases (General) Regulations 1986, as amended.

Individuals: regulatory liability 30.2

The FCA has continued the FSA's legacy of adopting a robust enforcement stance, underpinned by its 'credible deterrence' strategy. In furtherance of its policy of 'credible deterrence', the FSA had signalled a willingness to pursue criminal actions through the courts and to seek custodial sentences. For the FCA, the pursuit of criminal prosecutions, where appropriate, remains high on its agenda, particularly for market misconduct offences. This is supported by the FCA's Annual Business Plan for 2019/20, which states that tackling financial crime and money laundering remains a priority. The UK government's Economic Crime Plan 2019-22 also lists strengthening the capabilities of law enforcement as one of its strategic priorities, 'to detect, deter and disrupt economic crime'.[56] The FCA has introduced further changes to the Senior Managers and Certification Regime, due at the time of writing to come into force on 9 December 2019, extending the regime to FCA solo-regulated firms[57] to make senior managers more responsible and accountable for their actions.[58]

See Chapter 25 on fines, disgorgement, etc. and Chapter 41 on directors' duties

Under the Financial Services and Markets Act 2000 (FSMA) as amended by the Financial Services Act 2012, the FCA has many tools at its disposal to punish non-criminal offences and breaches. This includes the issuing of public censures or statements, and imposing unlimited financial penalties.

Other sanctions available to the FCA include varying or cancelling a firm's permission under Part 4A of FSMA; intervening against an incoming EEA or EU Treaty firm; suspending or restricting a firm's Part 4A permissions; suspending or restricting the approval given to an approved person; prohibiting an individual from performing regulated functions; withdrawing the approval of an approved person; and imposing a penalty on a person who has performed a controlled function without approval.

There will always be an element of publicity along with the imposition of such sanctions; however, public sanctions are certainly not the only way of dealing with cases of regulatory non-compliance. Taking into consideration the severity of an

56 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf.

57 'Solo-regulated firms' are firms that are regulated exclusively by the FCA rather than dually regulated by the FCA and Prudential Regulatory Authority. The regime will commence for benchmark administrators on 7 December 2020 to allow the FCA to carry out a dedicated consultation for benchmark administrators before making final rules for the sector.

58 https://www.fca.org.uk/firms/senior-managers-certification-regime/banking; https://www.fca.org.uk/publication/policy/ps18-14.pdf, accessed 18 November 2019.

offence, it may be satisfactorily addressed by using other remedial measures (for example, through the use of private warnings).

Chapter 6 of the FCA's Decision Procedure and Penalties manual (DEPP 6) contains the FCA's statement of policy in relation to the imposition and amount of penalties under FSMA.[59] DEPP 6A sets out its policy in relation to imposing suspensions or restrictions on firms and on approved persons. Chapter 7 of the FCA's Enforcement Guide sets out specific guidance on the FCA's powers in relation to financial penalties and public censures. Further, in April 2017, the FCA published an Enforcement Information Guide, which should be read in conjunction with DEPP and the Enforcement Guide.

See Chapter 25 on fines, disgorgement, etc.

30.3 Other issues: UK third-party rights

Section 393 FSMA gives third parties certain rights in relation to warning and decision notices given to another person in respect of whom the FCA is taking regulatory action. Where a warning notice has been given, section 393(1) provides that a third party prejudicially identified in the notice must be given a copy and a reasonable period to make representations on it.[60] No equivalent regime exists in the criminal sphere, where the DPA process (which involves the agreed statement of facts detailing the conduct of individuals) enables individuals to respond prior to the DPA being entered into.

Section 393(4) gives third-party rights in relation to a decision notice. It provides that a third party prejudicially identified in the notice must be given a copy of it and a reasonable period to make representations on it. Section 393(11) provides that a person who alleges that a copy of the notice should have been given to him or her may refer that alleged failure to the Upper Tribunal.[61]

The scope of the rights conferred by section 393(4) was reconsidered in *Macris v. FCA*.[62] On 19 May 2015, the Court of Appeal held that Mr Macris had been prejudicially identified in the FCA's settlement notices issued to a financial institution. Though he was not identified by name, the notices referred to him as 'CIO London management' and stated that 'CIO London management' had deliberately misled the FCA in a telephone call with the regulator in April 2012.

On 22 March 2017, the majority of the Supreme Court overturned the Court of Appeal's decision. Lord Sumption, writing for the majority, stated that someone is identified in a notice if 'he is identified by name or by a synonym for him, such as his office or job title'. Such a synonym would, in the view of Lord Sumption, need to be 'apparent from the notice itself that it could apply to only one person and that person must be identifiable from information which is either in the notice or publicly available elsewhere'. Information from other sources can

59 In August 2018, the FCA issued a new version of the DEPP.

60 Unless he or she has been given a separate warning notice in relation to the same matter.

61 In April 2010 the Financial Services and Market Tribunal, established by s.132 of FSMA as an independent judicial body to hear decision notices issued by the FSA, was abolished and its functions transferred to the Upper Tribunal.

62 [2015] EWCA Civ 490; [2017] UKSC 19.

only be used to interpret the language of the FCA's notice, rather than to supplement it, and must be easily ascertainable.

In concluding that it was not permissible to rely on information publicly available elsewhere, Lord Sumption stated that he was influenced by the deliberate drafting of section 393 FSMA with regard to fairness and the requirement for the material identifying the individual to come from the notice itself, as well as concern over the impact on the FCA's effectiveness if section 393 were to be interpreted differently. Lord Sumption also stated that the envisaged constituency, namely the audience of notices, was the public at large and not just those familiar with a particular industry.

While agreeing with Lord Sumption, Lord Neuberger stated that an individual is identified in a document if '(1) his position or office is mentioned, (2) he is the sole holder of that position or office, and (3) reference by members of the public to freely and publicly available sources of information would easily reveal the name of that individual by reference to his position or office.'

In dissenting, Lord Wilson stated that the majority unfairly prioritised protecting regulatory efficiency over individual reputation. Lord Wilson expressed concern about the majority's analysis that the general public is the constituency for FCA notices and stated that it failed to reflect how the most serious damage of wrongly being identified for a third party would be within the market in which they operate, as being so identified would damage their employment prospects. Lord Wilson considered that the decision failed to strike a balance between protecting the rights of individuals and regulatory efficiency. However, the restrictive approach to third-party rights has now been confirmed by the Court of Appeal in *R v. Grout*.[63]

63 [2018] EWCA Civ 71.

31

Individual Penalties and Third-Party Rights: The US Perspective

Joseph Moreno and Todd Blanche[1]

31.1 Prosecutorial discretion

31.1.1 Generally

In the United States, prosecutors generally have discretion in deciding whether to investigate and charge an individual with an offence.[2] As a threshold matter, a prosecutor may bring charges if there is probable cause to believe that the accused has committed a crime.[3] Prosecutors also have discretion as to how to charge a specific offence,[4] when to bring charges[5] and whether to negotiate a plea agree-

1 Joseph Moreno and Todd Blanche are partners at Cadwalader, Wickersham & Taft LLP.

2 See *United States v. Armstrong*, 517 U.S. 456, 464 (1996) (holding that the constitutional separation of powers requires broad prosecutorial discretion); *Young v. United States ex. Rel. Vuitton et Fils S.A.*, 481 U.S. 787, 807 (1987) (holding that prosecutors have discretion to decide which persons should be the target of an investigation); *Wayte v. United States*, 470 U.S. 598, 607 (1985) (finding that courts are ill equipped to evaluate the strength of a prosecutor's case, a case's deterrent value, and the government's enforcement priorities). See also American Bar Association, Criminal Justice Standards for the Prosecution Function (4th ed. 2018), Standard 3-4.2 (Decisions to Charge Are the Prosecutor's), www.americanbar.org/groups/criminal_justice/standards/ProsecutionFunctionFourthEdition-TableofContents.html.

3 See *Bordenkircher v. Hayes*, 434 U.S. 357, 364 (1978) (holding that, if a prosecutor has probable cause to believe that the accused committed an offence, the decisions whether to prosecute and what charges to file rest entirely within his discretion). See also *Rinaldi v. United States*, 434 U.S. 22, 29-30 (1977) (per curiam) (holding that the prosecutor has discretion to dismiss charges unless dismissal would be contrary to the public interest).

4 See *United States v. Batchelder*, 442 U.S. 114, 123-25 (1979) (holding that it is proper for prosecutors to bring charges under any statute unless brought for a discriminatory purpose).

5 See *United States v. Lovasco*, 431 U.S. 783, 795-96 (1977) (holding that an 18-month delay in bringing charges did not violate the defendant's due process rights).

ment.[6] Courts will typically not interfere with charging decisions absent a showing of selective prosecution[7] or vindictive prosecution.[8]

Principles of Federal Prosecution 31.1.2

Within the discretion provided to federal prosecutors, there is guidance issued by the Department of Justice (DOJ) to help with investigation and charging decisions.

The DOJ's Principles of Federal Prosecution – issued as part of the Justice Manual (JM) (formerly known as the US Attorneys' Manual, or USAM) – provide federal prosecutors with a framework for applying their prosecutorial discretion to 'promote the reasoned exercise of prosecutorial authority and contribute to the fair, evenhanded administration of the Federal criminal laws'.[9] They provide that if a prosecutor concludes that there is probable cause to believe that a person has committed a federal offence within the prosecutor's jurisdiction, the prosecutor should consider whether to (1) request or conduct further investigation, (2) commence or recommend prosecution, (3) decline prosecution and refer the matter for prosecutorial consideration in another jurisdiction, (4) decline prosecution and commence or recommend pretrial diversion or other non-criminal disposition, or (5) decline prosecution without taking other action.[10] A prosecutor should commence or recommend federal prosecution if he or she believes that the person's conduct constitutes a federal offence, and that the admissible evidence will probably be sufficient to obtain and sustain a conviction, unless (1) the prosecution would serve no substantial federal interest, (2) the person is subject to effective prosecution in another jurisdiction or (3) there exists an adequate non-criminal alternative to prosecution.[11]

In determining whether a prosecution 'would serve a substantial federal interest', the Principles of Federal Prosecution advise prosecutors to weigh all relevant considerations, including (1) federal law enforcement priorities, including any federal law enforcement initiatives or operations aimed at accomplishing those priorities, (2) the nature and seriousness of the offence, (3) the deterrent effect of prosecution, (4) the person's culpability in connection with the offence, (5) the person's history with respect to criminal activity, (6) the person's willingness to co-operate in the investigation or prosecution of others, (7) the person's

6 See *Weatherford v. Bursey*, 429 U.S. 545, 561 (1977) (holding there is no constitutional right to plea bargain).

7 See *Yick Wo v. Hopkins*, 118 U.S. 356, 373-74 (1886) (selective prosecution of Chinese laundry owners but not similarly situated non-Chinese laundry owners).

8 See *Blackledge v. Perry*, 417 U.S. 21, 28-29 (1974) (prosecution of a defendant for a more serious charge in a new trial following a successful appeal of his original conviction).

9 Justice Manual (JM), Principles of Federal Prosecution, § 9-27.000 et seq., https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution.

10 Id., at § 9-27.200 (Initiating and Declining Prosecution – Probable Cause Requirement).

11 Id., at § 9-27.220 (Grounds for Commencing or Declining Prosecution).

circumstances, (8) the interests of any victims, and (9) the probable sentence or other consequences if the person is convicted.[12]

The Principles of Federal Prosecution also establish important boundaries as to what a prosecutor should not consider when determining whether to bring charges against an individual, including (1) the person's race, religion, gender, ethnicity, national origin, sexual orientation, or political association, activities or beliefs, (2) the prosecutor's own personal feelings concerning the person, the person's associates or the victim, or (3) the possible effect of the decision on the prosecutor's own professional or personal circumstances.[13]

31.1.3 DOJ enforcement priorities and policies

The first factor within the Principles of Federal Prosecution for prosecutors to consider – federal law enforcement priorities – are developed annually by the DOJ to focus efforts on those matters that are most deserving of federal attention. Every year, the Attorney General communicates the DOJ's national enforcement priorities, which have ranged from a focus on drug prosecutions during the influx of crack cocaine in the 1980s, to national security and counterterrorism following the attacks of 11 September 2001, and to prosecuting mortgage and financial fraud in the wake of the Wall Street credit crisis of 2008.[14]

In addition, the DOJ periodically issues policy guidance that has an impact on prosecutorial discretion, frequently corresponding to changes in DOJ leadership. For example, on 10 May 2017, then-Attorney General Jeff Sessions issued a memorandum to all federal prosecutors entitled 'Department Charging and Sentencing Policy', which directed that 'prosecutors should charge and pursue the most serious, readily provable offence.'[15] In addition, the memorandum directed prosecutors to disclose to the court 'all facts that impact the sentencing guidelines or mandatory minimum sentences'.[16] By this memorandum, the Attorney General modified charging policies then in effect, limiting prosecutors' discretion in making charging decisions and sentencing recommendations and requiring any exceptions to be approved by the respective US Attorney.[17] The use of these memoranda by the DOJ leadership is another mechanism by which policy changes are put into effect.

12 Id., at § 9-27.230 (Initiating and Declining Charges – Substantial Federal Interest).

13 Id., at § 9-27.260 (Initiating and Declining Charges – Impermissible Considerations).

14 See, e.g., US Department of Justice, press release, 'Department of Justice FY 2020 Budget Request' (11 March 2019), https://www.justice.gov/opa/pr/department-justice-fy-2020-budget-request (listing drug enforcement and the opioid crisis, combating violent crime, immigration law enforcement, and national security and cyber as among the DOJ's federal law enforcement priorities for Fiscal Year 2020).

15 Office of the Attorney General, US Department of Justice, Department Charging and Sentencing Policy (10 May 2017), https://www.justice.gov/opa/press-release/file/965896/download.

16 Id.

17 In February 2018, the DOJ amended JM § 9-27.300 (Selecting Charges– Charging Most Serious Offences) to incorporate the May 2017 Sessions Memo stating that federal prosecutors must pursue the most serious offences that carry the most substantial Guidelines sentence.

Individual accountability for wrongdoing 31.1.4

Under US law, criminal prosecution and civil actions may be brought against business organisations including corporations, partnerships, sole proprietorships, government entities and other unincorporated associations, notwithstanding their artificial nature as a legal entity.[18] The prosecution of corporate crime has long been a high priority for the DOJ, with a focus on (1) protecting the integrity of the economic and capital markets by enforcing the rule of law, (2) protecting consumers, investors and business entities against competitors who gain unfair advantage by violating the law, (3) preventing violations of environmental laws and (4) discouraging business practices that would permit or promote unlawful conduct at the expense of the public interest.[19] Under this concept of corporate liability, corporations and other business organisations can be indicted, plead guilty, be convicted of offences, be fined and be required to institute remedial measures to prevent future wrongdoing.[20] Just as prosecutors have discretion in deciding when, how, and whether to prosecute individuals, they have similar latitude in prosecuting and negotiating settlements with corporate defendants.[21]

Historically, the DOJ's focus on corporate wrongdoing often led to significant settlements with companies, but without any individuals being held accountable for the crimes charged. Following increasing public and judicial criticism about the lack of individual accountability, in September 2015, the DOJ issued a memorandum titled 'Individual Accountability for Corporate Wrongdoing', authored by then-Deputy Attorney General Sally Quillian Yates (commonly referred to as the Yates Memorandum).[22] The Yates Memorandum set forth new policy guidance focusing on prosecuting individuals with responsibility for the crimes for which corporations could be held responsible, and its core principles were incorporated into the USAM several months later. In acknowledging the historical challenge of identifying and prosecuting individuals who were aware of or complicit in corporate misconduct, the Yates Memorandum listed six key steps to strengthen the DOJ's pursuit of individual wrongdoers.

- *Provision of evidence against individual wrongdoers*: For a company to receive any consideration for co-operation with the government under the Principles of Federal Prosecution of Business Organizations, the company must completely disclose to the DOJ all relevant facts about any individual misconduct. This includes identifying all individuals responsible for the misconduct at issue, regardless of their position, status or seniority at the company.

18 JM, Principles of Federal Prosecution of Business Organizations, § 9-28.000 et seq., https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.

19 Id., at § 9-28.010 (Foundational Principles of Corporate Prosecution).

20 Id., at § 9-28.200 (General Considerations of Corporate Liability).

21 Id.

22 Office of the Deputy Attorney General, US Department of Justice, Individual Accountability for Corporate Wrongdoing (9 September 2015), https://www.justice.gov/dag/file/769036/download. The Yates Memorandum has since been largely incorporated into JM § 9-28.700 (The Value of Cooperation).

- *Investigative focus on individual wrongdoers*: Both civil attorneys and criminal prosecutors at the DOJ will now focus on individual wrongdoing from the beginning of any investigation of corporate misconduct.
- *Coordination between civil attorneys and criminal prosecutors*: Civil attorneys and criminal prosecutors at the DOJ will more regularly consult throughout all phases of an investigation of corporate misconduct and will consider bringing parallel civil and criminal proceedings to take advantage of the full range of the government's potential remedies, including fines, imprisonment, forfeitures, restitution, and suspension and debarment.
- *No shielding of individuals from liability*: Absent extraordinary circumstances, no resolution of a case of corporate misconduct will provide protection from criminal or civil liability for individuals. Any release of criminal or civil liability due to extraordinary circumstances must be personally approved in writing by the relevant Assistant Attorney General or United States Attorney.
- *No corporate resolution without individual resolution*: If the investigation of individual misconduct has not concluded by the time authorisation is sought to resolve the case against the corporation, a plan must be implemented by the DOJ prosecutor on how to resolve the matter prior to the end of any statute of limitations period.
- *Increased focus on civil settlements*: Civil attorneys at the DOJ will focus on recovering as much money as possible for the public, regardless of an individual's ability to pay. Instead, the decision as to whether to file a civil action against an individual should focus on the seriousness of the person's misconduct, whether it is actionable, whether the admissible evidence will be sufficient to obtain a judgment and whether pursuing the action reflects an important federal interest.

To some practitioners, the Yates Memorandum merely memorialised the DOJ's existing practice of prosecuting culpable individuals in white-collar cases. However, the requirement that the government prove that defendants intentionally and knowingly violated the law remains a significant hurdle, especially in the context of corporate wrongdoing. Indeed, the Yates Memorandum notes that in cases of misconduct in a large corporate setting 'where responsibility can be diffuse . . . it can be difficult to determine if someone possessed the knowledge and criminal intent necessary to establish their guilt beyond a reasonable doubt.'[23]

In November 2018, then-Deputy Attorney General Rod Rosenstein announced revisions to the Yates Memorandum to restore some of the prosecutorial discretion that had traditionally been afforded to cases involving corporate wrongdoing.[24] Rosenstein's speech, while emphasising that the aggressive target-

23 Ibid.

24 Deputy Attorney General Rod J Rosenstein Delivers Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

ing of white-collar crime in general and individuals in particular remained a 'top priority', also effectively conceded that the Yates Memorandum's 'all or nothing' approach was somewhat unrealistic. In deviating from a position whereby corporations must identify every individual wrongdoer to obtain co-operation credit, Rosenstein stated that the new policy permits prosecutors to recognise credit when a corporation identifies the individuals who play 'significant roles' in corporate misconduct. The revised policy allowed prosecutors more discretion to agree to credit based on the extent of a corporation's co-operation, while maintaining the position that corporations that failed to co-operate in good faith would remain ineligible for credit.[25] The effective components of the Yates Memorandum, as revised by the Rosenstein comments, have been incorporated into the Justice Manual.[26]

Sentencing 31.2

Generally 31.2.1

Individuals who are convicted of violating a federal criminal law, including white-collar laws, face a range of possible punishments including fines, probation and imprisonment. In determining the nature and range of a potential sentence following a conviction, there are currently two sources of guidance for judges, prosecutors and defence counsel to refer to: criminal statutes in the United States Code[27] and the United States Sentencing Guidelines (the Guidelines).[28]

Prior to 1984, federal judges had broad discretion in sentencing criminal defendants up to and including imprisonment, subject only to mandatory minimum or maximum sentences set forth in individual criminal statutes. Certain criminal statutes contain mandatory minimum sentences – for example, aggravated identity theft is punishable by a mandatory minimum sentence of imprisonment for two years, or by a mandatory term of imprisonment for five years if it relates to a terrorism offence.[29] Drug trafficking offences typically involve mandatory minimum sentences depending on the nature and quantity of the controlled substance involved and the defendant's criminal history.[30] Other statutes establish maximum terms of imprisonment, or a combination of a fine and imprisonment, such as bank fraud, which is punishable by a fine or a term of imprisonment of not more than 30 years.[31] Not surprisingly, these broad sentencing parameters often resulted in wide sentencing disparities across jurisdictions for similar conduct.[32]

25 Ibid.

26 JM § 9-28.700 (The Value of Cooperation).

27 United States Code (U.S.C.), US Government Publishing Office, https://www.govinfo.gov/app/collection/uscode/.

28 US Sentencing Guidelines Manual (effective 1 November 2018), United States Sentencing Commission, https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2018/GLMFull.pdf.

29 18 U.S.C. § 1028A.

30 See, e.g., 21 U.S.C. § 841(b).

31 18 U.S.C. § 1344.

32 See US Sentencing Commission, Supplementary Report on the Initial Sentencing Guidelines and Policy Statements 35-39 (18 June 1987), https://www.ussc.gov/sites/default/files/pdf/

In response, Congress passed the Sentencing Reform Act of 1984 (SRA), which led to the creation of the Guidelines.[33] The Guidelines require a score-based analysis focused on a myriad of factors relating to the circumstances of the offence. This analysis leads to one of 43 different offence levels[34] and six criminal history categories.[35] As originally designed, the Guidelines were mandatory. A sentencing judge was required to apply a sentence from within the Guideline range dictated by the score-based analysis. However, in 2006, the US Supreme Court in *United States v. Booker* determined that mandatory application of the Guidelines was unconstitutional and that they are advisory recommendations only.[36] As a result of *Booker*, the Guidelines now act as a starting point for a federal judge to determine what sentence should be imposed, consistent with minimum and maximum sentences set forth in the offence of conviction, as well as the factors set forth in the federal sentencing statute.[37] Notably, while a judge is required to consider the Guidelines when determining an appropriate sentence, it is but one of many factors that the judge must consider when determining an appropriate sentence.

guidelines-manual/1987/manual-pdf/1987_Supplementary_Report_Initial_Sentencing_Guidelines.pdf.

33 18 U.S.C. §§ 3551-3586, 3601-3742; 28 U.S.C. §§ 991-998. The Sentencing Reform Act of 1984 (SRA) required a federal district court judge to consider each of the factors in the federal sentencing statute, 18 U.S.C. § 3553(a), when crafting a sentence, which included: (1) the 'nature and circumstances of the offence' and the defendant's 'history and characteristics'; (2) the general purposes of the SRA; (3) the 'kinds of sentences available'; (4) the 'pertinent policy statements issued by the U.S. Sentencing Commission'; (5) the 'need to avoid unwarranted sentence disparities' between defendants convicted of similar conduct; (6) the 'need to provide restitution to any victims'; and (7) the applicable sentence range recommended by the Guidelines.

34 Guidelines § 5A.

35 Guidelines § 4A1.1.

36 543 U.S. 220, 245-246 (2005) (holding that the Guidelines must be considered as an advisory, not a mandatory, calculation of sentence to be consistent with the Sixth Amendment right to a trial by jury). The *Booker* court held that the federal sentencing statute requires judges to consider the Guidelines sentencing range, and to 'impose sentences that reflect the seriousness of the offense, promote respect for the law, provide just punishment, afford adequate deterrence, protect the public, and effectively provide the defendant with needed educational or vocational training and medical care.' Ibid., at 259, 260 (citing 18 U.S.C. § 3553(a)).

37 18 U.S.C. § 3553(a). The federal sentencing statute defines the factors to be considered by the judge in imposing a sentence on a defendant and mandates that it should be 'sufficient, but not greater than necessary'. 18 U.S.C. § 3553(a)(2). As a result of the Supreme Court's ruling in *Booker*, courts should consider the Guidelines as one factor in imposing a sentence, but a judge may impose a different sentence if other § 3553(a) factors suggest that the Guidelines' range is inappropriate. See *Kimbrough v. United States*, 552 U.S. 85, 91 (2007). ('A district judge must include the Guidelines range in the array of factors warranting consideration.')

Imprisonment 31.2.2

The federal prison system is operated by the Bureau of Prisons, and currently contains over 177,000 inmates in over 140 facilities located throughout the United States.[38]

When calculating a potential sentence of imprisonment under the Guidelines, the judge first looks to the 'base offence level' applicable to the defendant's conviction,[39] and adjusts that upward or downward for specific applicable offence characteristics, special instructions and other factors to calculate the 'total offence level'.[40] Next, the judge determines the defendant's criminal history category (categories I to VI), which is increased by prior criminal convictions.[41] Once the total offence level and criminal history category are determined, the judge arrives at the recommended sentence by identifying the applicable range in the Guidelines' sentencing table.[42] Judges have discretion to depart upward or downward from the recommended range upon finding that the case includes one or more aggravating or mitigating circumstance 'of a kind not adequately taken into consideration' by the Guidelines.[43] They also allow judges to depart from the Guidelines if the government moves for a downward departure based on the defendant's substantial assistance in another case.[44] In any case, the judge must state in writing the specific reasons for imposing a sentence outside the applicable Guidelines sentencing range.[45]

Fines 31.2.3

An individual convicted of a federal crime may also be sentenced to pay a monetary fine.[46] The process a judge uses to calculate an applicable fine is similar to that of determining a sentence of imprisonment. Many criminal statutes set forth the range of fines that may be assessed upon conviction; for those felonies whose statute does not so specify, the fine is set at not more than US$250,000.[47] As with terms of imprisonment, the Guidelines contain a fine table that provides the court with an advisory minimum and maximum fine range for defendants, based on the offence level at which the defendant is sentenced.[48]

Judges may depart upwards or downwards from the Guidelines' fine range based on factors such as a defendant's ability to pay, any restitution the defendant

38 Federal Bureau of Prisons Statistics (updated 25 July 2019), https://www.bop.gov/about/statistics/population_statistics.jsp.

39 Guidelines §§ 1B1.1(a)(1), 1B1.2(a).

40 Guidelines §§ 1B1.1(a)(2), 1B1.1(c).

41 Guidelines § 1B1.1(a)(6).

42 Guidelines § 1B1.1(a)(7).

43 Guidelines § 5K2.0 (quoting 18 U.S.C. § 3553(b)).

44 Guidelines § 5K1.1.

45 18 U.S.C. § 3553(c)(2).

46 18 U.S.C § 3571(a).

47 18 U.S.C § 3571(b)(3).

48 Guidelines § 5E1.2. For example, if a defendant is convicted of bank fraud and is sentenced at offence level 18, the fine table sets a guideline range of US$6,000 to US$60,000. Ibid.

must make, the potential for collateral consequences the defendant may face (such as civil litigation) and other equitable considerations.[49] Judges looking to assess a fine should also consider the factors in the federal sentencing statute in calculating the amount, including the seriousness of the offence, promotion of respect for the law, provision of just punishment for the defendant and its deterrent factor.[50]

31.2.4 Probation

The US Probation and Pretrial Services System supervises individuals sentenced to a term of probation to ensure compliance with conditions imposed by the sentencing judge. Probation is a sentence in and of itself, and may be used as an alternative to imprisonment.[51] When imposing probation, the sentencing judge must consider the Guidelines[52] as well as the factors set forth in the SRA.[53]

The Guidelines contain a list of standard conditions that are recommended in all cases of probation,[54] along with a list of special conditions to be considered under certain circumstances.[55] In addition, a judge may impose additional conditions on a defendant's probation term that are reasonably related to the nature and circumstances of the offence, the history and characteristics of the defendant, and the goals of sentencing.[56] In all cases, the court must provide the defendant with written notice of the conditions.[57] The court may revoke a defendant's probation at any time before the end of its term for any violation of a probation condition that occurs during that time.[58]

31.2.5 Confiscation of assets

31.2.5.1 Pretrial asset freeze orders

Under US law, the government can seek a temporary order freezing an individual's assets, in both the civil and criminal contexts, before a case is proven at trial. In civil enforcement matters, regulators can seek asset freezes from an administrative

49 Guidelines § 5E1.2(d).

50 See 18 U.S.C. § 3553(a).

51 18 U.S.C. § 3561; Guidelines § 5B1.1.

52 See, e.g., *United States v. Toohey*, 448 F.3d 542, 546-47 (2d Cir. 2006) (holding that a departure from the Guidelines' prison recommendation to probation may be warranted, but the district court should nonetheless 'consider the Guidelines and all of the other factors listed in § 3553(a)').

53 The SRA directs the sentencing judge, when imposing probation, to consider several factors, including: (1) the nature of the offence and history and characteristics of the defendants; (2) the need for just punishment, deterrence, or public protection; (3) the need to provide the defendant with educational or vocational training, medical care, or other correctional treatment; (4) the types of sentences available; (5) the Guidelines; (6) the need to avoid unwarranted sentencing disparities between defendants with similar records for similar conduct; and (7) the need to provide restitution to victims. See 18 U.S.C. § 3553(a).

54 Guidelines § 5B1.3(c).

55 Guidelines §§ 5B1.3(d), (e).

56 Guidelines § 5B1.3(b).

57 18 U.S.C. § 3563(d).

58 18 U.S.C. § 3564(e), 3565(a).

law judge once an action is initiated, often in *ex parte* proceedings at which the respondent is not present. In criminal matters, prosecutors can seek asset freeze orders from a district court based on a showing of probable cause that the assets are subject to permanent forfeiture.

In the past, courts were unconvinced by the constitutional argument that pretrial asset freeze orders were a violation of a defendant's Sixth Amendment right to counsel, even if those assets would otherwise be used to pay lawyers' fees.[59] However, more recently, the Supreme Court in *Luis v. United States* held that the pretrial restraint of a criminal defendant's assets – which assets were not 'tainted' by the alleged criminal conduct – violates the Sixth Amendment right to counsel.[60] As a result, while the government can freeze and seize assets pretrial that are believed to derive from criminal activity, its ability do so for 'untainted' assets are trumped by the defendant's Sixth Amendment right to counsel of choice.

Civil and criminal asset forfeitures 31.2.5.2

Permanent government confiscation of property is called a 'forfeiture'. There are generally three types of forfeiture proceedings available to US law enforcement and prosecutors: administrative, civil and criminal.[61]

Administrative forfeiture permits a federal agency to seize personal (non-real) property without initiating a judicial proceeding. The authority derives from the Tariff Act of 1930, which states that the following types of property are eligible for administrative forfeiture: (1) property whose value does not exceed US$500,000; (2) merchandise whose importation is prohibited; (3) a conveyance used to import, transport or store a controlled substance; or (4) a monetary instrument.[62]

The deadlines and notice requirements for the various types of administrative forfeiture proceedings are set forth in the Civil Asset Forfeiture Reform Act of 2000.[63] Once property is administratively seized, the federal agency involved must give written notice of the seizure to each party who appears to have an interest in the seized article.[64] The notice must contain a description of the property seized; the time, cause and place of the seizure; how a person seeking to claim the property should proceed; and, if known, the name and residence of the owner of the seized property.[65] If no one contests the administrative forfeiture within the dead-

59 See *Caplin & Drysdale v. United States*, 491 U.S. 617, 626 (1989) (holding that '[a] defendant has no Sixth Amendment right to spend another person's money for services rendered by an attorney'); *United States v. Monsanto*, 491 U.S. 600, 615 (1989) (holding that the right to counsel was not violated when a defendant's assets were frozen pre-conviction).

60 136 S. Ct. 1083 (2016).

61 The DOJ's Asset Forfeiture and Money Laundering Section publishes an Asset Forfeiture Policy Manual, most recently updated in 2019, to set forth DOJ policy and provide guidance to US Attorneys' Offices on the DOJ's Asset Forfeiture Program. See Asset Forfeiture Policy Manual, available at https://www.justice.gov/criminal-afmls/file/839521/download.

62 19 U.S.C. § 1607.

63 Pub. L. No. 106-185, 114 Stat. 202 (2000).

64 19 U.S.C. § 1607(a).

65 19 C.F.R. § 162.45.

line specified, claimants lose their ability to contest the forfeiture. If a timely claim of the property is received, the matter is referred to the United States Attorney's Office for a judicial proceeding.

Civil forfeiture is an *in rem* proceeding that is brought directly against a piece of real or personal property that is involved, derived from or traceable to one or more enumerated federal crimes.[66] The property itself is the defendant and no charge against an individual is necessary. In a civil forfeiture proceeding, the government must prove, by a preponderance of the evidence, that the property is subject to forfeiture.[67] If a claimant raises an innocent owner defence, he or she has the burden of proving that the claimant is an innocent owner of the property by a preponderance of evidence.[68]

Criminal forfeiture is an action brought as part of a criminal case against a defendant, not against a specific asset. It is an *in personam* action and requires the government to include a forfeiture charge against the defendant in the indictment, and prove that the property was used or derived from one or more enumerated federal crimes.[69] The indictment or criminal information must contain notice to the defendant that the government is seeking forfeiture of property as part of any sentence.[70] If a defendant disposes of the original asset subject to forfeiture, the government may obtain substitute assets[71] or may obtain a money judgment in an amount equal to the criminal proceeds.

When a criminal defendant is found guilty on charges that include the potential criminal forfeiture of property, in most cases the jury then determines whether the government has established 'the requisite nexus between the property and the offense committed by the defendant'.[72] If so, a preliminary order of forfeiture is entered against the defendants. If there are any third parties with an interest in the property, they may seek an ancillary proceeding to prevent the seizure by the government.[73] After the trial judge has disposed of any third-party claims, a final order of forfeiture is entered and the defendant's interest in the property is divested.[74]

A defendant can challenge the dollar amount of a criminal or civil forfeiture as a violation of the Eighth Amendment to the US Constitution, which restricts

66 18 U.S.C. §§ 981 and 983-5.

67 18 U.S.C. § 982(c)(91).

68 18 U.S.C. § 982(d)(1).

69 18 U.S.C. § 982.

70 Fed. R. Crim. P. 32.2(a).

71 Prosecutors may seek the forfeiture of 'substitute assets' in place of tainted property when certain conditions are met. See 21 U.S.C. § 853(p) (incorporated by reference in various criminal forfeiture statutes).

72 Fed. R. Crim. P. 32.2(b)(4). See *Honeycutt v. United States*, 137 S. Ct. 1626 (2017) (rejecting lower court findings allowing joint and several liability for forfeiture among members of a criminal conspiracy, and holding that criminal asset forfeiture statutes are 'limited to property the defendant himself actually acquired as the result of the crime').

73 Fed. R. Crim. P. 32.2(c).

74 Fed. R. Crim. P. 32.2(c)(2).

the government's ability to impose 'excessive fines' as punishment.[75] Among other factors, courts conducting such a review will look to whether the forfeiture is disproportionate to the defendant's conduct and, therefore, excessive.[76]

Compensation orders 31.2.6

Under the Mandatory Victims Restitution Act of 1996,[77] defendants convicted of certain federal crimes, as well as defendants sentenced to probation, must in most circumstances make restitution to each of their victims in the full amount of the victim's financial losses that resulted from the defendant's crimes.[78] Restitution by the defendant must be ordered regardless of the defendant's economic circumstances, or any third-party compensation received by the victim.[79] Judges must, however, consider a defendant's economic circumstances when deciding on a payment schedule and form of restitution.[80]

Judges must reduce a restitution amount to be paid to a victim if the victim recovers compensatory damages from the defendant for the same loss in a civil proceeding.[81] In addition, if a victim has received insurance proceeds as compensation for a loss suffered due to the defendant's crimes, the defendant's restitution must be paid to the insurance company.[82]

Disqualification and other consequential orders 31.2.7

In addition to imprisonment, fines, probation, forfeitures and other direct sanctions that may be imposed by a criminal court, there are a number of other federal, state and local legal and regulatory restrictions that may result as 'collateral

75 See *Alexander v. United States*, 509 U.S. 544, 558-59 (1993) (holding that the excessive fines clause of the Eighth Amendment applies to in personam criminal forfeiture for purposes of determining whether a penalty is 'excessive'); Austin v. United States, 509 U.S. 602, 609, 610 (1993) (holding that the excessive fines clause applies to civil forfeitures of conveyances and real property used to facilitate the transport, sale, or possession of controlled substances under 21 U.S.C. §§ 881(a)(4) and (7)).

76 See *Alexander*, 509 U.S. at 558, 559.

77 Pub. L. No. 104-132, § 204, 110 Stat. 1214, 1227 (codified at 18 U.S.C. §§ 3556, 3663 and 3664).

78 See *Hughey v. United States*, 495 U.S. 411, 413 (1990) (holding that restitution may only be awarded for losses resulting from the specific conduct for which the defendant was convicted). The *Hughey* decision was subsequently modified by Congress pursuant to the Crime Control Act of 1990, which authorised courts to order any restitution amount agreed to in a plea agreement, and broadened restitution payable to any person directly harmed by the defendant's conduct in the course of a scheme or conspiracy. See Pub. L. No. 101-647 § 2509, codified at 18 U.S.C. § 3663. See also *Lagos v. United States*, 138 S. Ct. 1684 (2018) (limiting the ability of corporate victims to obtain restitution orders for legal fees and other costs incurred in conducting internal investigations into a defendant's misconduct).

79 18 U.S.C. § 3664(f)(1)(A)-(B).

80 18 U.S.C. § 3664(f)(2).

81 18 U.S.C. § 3664(j)(2).

82 18 U.S.C. § 3664(j)(1).

consequences' of a criminal conviction.[83] These are opportunities and benefits that are no longer fully available to a person, or legal restrictions a person may operate under, because of their criminal conviction. They are imposed automatically upon conviction, even if not expressly included in the criminal court's judgment, or by action of a civil court or administrative agency. Examples of collateral consequences of a criminal conviction include (1) disqualification from jury service and loss of voting rights, (2) ineligibility for federal employment or military service, (3) inability to obtain a passport or possess a firearm, (4) being banned from serving as an officer or director of a public company, and (5) (for individuals with professional licences, such as attorneys, certified public accountants and securities brokers) suspension or loss of licence.

An individual's suspension or debarment from government contracting is another potential consequence of a criminal proceeding. Allegations of fraud, theft, bribery, falsification of records, violating federal law or other misconduct can all lead to limiting a contractor's ability to do business with federal government agencies. This could begin as a suspension, which is a temporary measure limited to 12 months' duration, that may be imposed at the beginning of an investigation or at the time of criminal indictment. Upon conviction, a contractor may face debarment, which typically means a three-year ban as well as public notification that the contractor is ineligible for government procurement and non-procurement programmes during that time. The relevant agency has a process for considering suspensions and debarments, and while contractors have certain rights to respond and meet the federal personnel considering the matter, the ultimate decision is made at the agency level. Either situation could lead to significant economic consequences for a business that depends on government contracts to survive.

83 See ABA Standards for Criminal Justice, Collateral Sanctions and Discretionary Disqualification of Convicted Persons, Standards 19-2.1 and 19-3.1 (3d ed. 2003), https://www.americanbar.org/groups/criminal_justice/publications/criminal_justice_section_archive/crimjust_standards_collateral_blk/#2.1.

32

Monitorships

Richard Lissack QC, Nico Leslie, Christopher J Morvillo, Tara McGrath and Kaitlyn Ferguson[1]

Introduction 32.1

In the United States, the past decade has seen a notable increase in the use of independent corporate monitors in connection with the resolution of corporate criminal and regulatory investigations. This trend has also recently found a statutory foothold in the United Kingdom, after a period of sporadic sampling of use of corporate monitorships as a tool in the sentencing armoury. Now, in the wake of the United Kingdom's deferred prosecution agreement regime, it is safe to assume that the appointment of a monitor will increasingly feature in the settlement and disposal of corporate investigations. Although monitors come in many shapes and sizes, they typically help to create and supervise the implementation of compliance and remediation programmes to address the perceived deficiencies that gave rise to the wrongdoing. It is expected that monitors will reduce recidivism for corporate misconduct, benefiting the corporation, its shareholders and the public.

In the United States, monitors have been used in both the civil and criminal contexts, typically in conjunction with a settlement agreement negotiated between the parties to a dispute, and often with the approval and supervision of the courts.[2] Outside the criminal context, monitors have been used as conditions

1 Richard Lissack QC and Nico Leslie are members of Fountain Court Chambers. Christopher J Morvillo is a partner, and Tara McGrath and Kaitlyn Ferguson are associates, at Clifford Chance US LLP.

2 In 2014, for instance, the Department of Justice entered into a civil settlement with Citigroup that included a monitorship provision to address Citigroup's false representations to investors regarding its residential mortgage-backed securities. See Department of Justice (DOJ) press release, 'Federal and State Partners Secure Record $7 Billion Global Settlement with Citigroup for Misleading Investors About Securities Containing Toxic Mortgages' (14 July 2014). Monitors may also be used in private cases, especially where there are concerns that misconduct may reoccur

of settlements between business entities and a wide range of federal and state agencies,[3] as well as international bodies such as the World Bank.[4] Even private litigants have included monitors in their settlement agreements.[5]

Yet the prevalence of monitors as a condition of high-profile corporate criminal resolutions sets the stage for close scrutiny of the practice in the United States and has given rise to congressional hearings, several United States Department of Justice (DOJ) policy enactments, legal challenges and the promulgation of bar association standards. Therefore, this chapter will focus on monitors used in conjunction with the resolution of federal criminal investigations conducted by the DOJ (including, of course, the various United States Attorney's Offices).[6] Because the practice of using monitors is relatively new in the United Kingdom, this chapter will draw parallels and contrasts in UK law and practice where appropriate from the more developed US practice. After briefly discussing the history of corporate monitors in both countries, this chapter will analyse certain key issues surrounding the use of monitors in both jurisdictions, including the appointment, roles, supervision and funding of monitors.

---

or an institution's culture needs to be remodelled to ensure future compliance. See, e.g., Athletics Integrity Agreement between the National Collegiate Athletic Association and The Big Ten Conference, and the Pennsylvania State University (29 August 2012), available at www.psu.edu/ur/2012/Athletics_Integrity_Agreement.pdf; NCAA, Former Sen. Mitchell Selected as Penn State Athletics Integrity Monitor (1 August 2012), www.ncaa.org/about/resources/media-center/news/former-sen-mitchell-selected-penn-state-athletics-integrity.

3 The Environmental Protection Agency and Securities and Exchange Commission, among many others, also use monitors as part of settlements. See, e.g., Environmental Protection Agency News Release, Duke Energy Subsidiaries Plead Guilty and Sentenced for Clean Water Act Crimes (14 May 2015) (noting that various Duke Energy subsidiaries would be 'monitored by an independent court[-]appointed monitor'); DOJ press release, 'Taiwan-Based AU Optronics Corporation Sentenced to Pay $500 Million Criminal Fine for Role in LCD Price-Fixing Conspiracy' (20 September 2012) (discussing a court-appointed monitor in the antitrust matter against AU Optronics Corporation); Seth Schiesel and Simon Romero, 'WorldCom Strikes a Deal with SEC', *N.Y. Time*s (27 November 2002), www.nytimes.com/2002/11/27/business/worldcom-strikes-a-deal-with-sec.html (discussing WorldCom's settlement with the SEC, which included a monitorship).

4 As part of the World Bank Sanctions Procedures, an independent monitor may be required for parties seeking to remain active with the Bank. World Bank Sanctions Procedures § 9.03 (15 April 2012), available at http://siteresources.worldbank.org/EXTOFFEVASUS/Resources/WBGSanctions_Procedures_April2012_Final.pdf.

5 See, e.g., NCAA Appointed Integrity Monitor, supra note 2, at 1. Additionally, monitors are frequently appointed in lawsuits between private plaintiffs and the government. For example, a monitor was appointed as part of the City of New York's settlement with private plaintiffs regarding the police department's discriminatory enforcement of anti-trespassing rules. Memorandum Opinion and Order at 3 n.8, *Davis v. City of New York*, No. 10 Civ. 0699 (S.D.N.Y. 28 April 2015).

6 Unless otherwise specified, references herein to 'monitors' or 'monitorships' concern DOJ/United States Attorney's Offices (USAO) corporate monitorships.

Evolution of the modern monitor 32.2

United States 32.2.1

Most monitorships arise as a result of a corporate guilty plea, deferred prosecution agreement (DPA) or non-prosecution agreement (NPA).[7] The DOJ first used DPAs and NPAs in 1993,[8] with the first recognised monitorship following in 1995, in connection with Consolidated Edison's sentencing for disclosure failures following a deadly steam pipe explosion.[9] Spurred on by the collapse of Enron in 2001 and other high-profile instances of corporate misconduct, the US federal government prioritised and increased the investigation and prosecution of corporations. This increase naturally led to a growth in the number of corporate guilty pleas, DPAs and NPAs, and, concomitantly, the rise of monitorships as a condition of settlement.

See Chapters 9 and 10 on co-operating with authorities and Chapters 23 and 24 on negotiating global settlements

As the frequency of monitorships has increased, so too has their level of scrutiny. One of the most controversial aspects of monitorships has been monitor selection. The issue received considerable attention in 2007 when Chris Christie – then the US Attorney for the District of New Jersey – approved, without a bidding process, a contract for a consulting firm founded by his former boss, Attorney General John Ashcroft, to serve as the monitor for medical device company Zimmer Holdings (a contract reportedly worth between US$28 million and US$52 million in monitor fees).[10] Concerns of cronyism, transparency and conflicts of interest led the US Congress to hold an investigative hearing to better understand the appointment.

---

7 DPAs and NPAs, while similar in that they are both pretrial settlement options available to the DOJ/USAO, have different collateral consequences for corporate defendants. With a DPA, the DOJ files a criminal information, which under the DPA the DOJ agrees to dismiss after a term of months or years if the corporate defendant complies with all other terms of the settlement. DPAs are, by virtue of being filed with a court, publicly available and therefore subject corporate defendants to adverse public relations and scrutiny. By contrast, with a NPA, the government agrees not to bring charges against the corporate defendant if it complies with the terms of the settlement; NPAs are not required to be disclosed, though they frequently are by the corporate defendant and/or the DOJ. Because NPAs do not involve the courts, they tend to be far more flexible and desirable for corporate defendants than DPAs.

8 See US Gov't Accountability Off., GAO-10-260T, Prosecutors Adhered to Guidance in Selecting Monitors for Deferred Prosecution and Non-Prosecution Agreements, But DOJ Could Better Communicate Its Role in Resolving Conflicts (2009).

9 See James C McKinley, 'Con Ed Fined and Sentenced to Monitoring for Asbestos Cover-Up', *N.Y. Times* (22 April 1995), www.nytimes.com/1995/04/22/nyregion/con-ed-fined-and-sentenced-to-monitoring-for-asbestos-cover-up.html. Note, the DOJ was not the first government agency to use monitors. Monitors were used as early as 1978 by the SEC. SEC News Digest, Issue 80-71 at 3 (10 April 1980), available at https://www.sec.gov/news/digest/1980/dig041080.pdf (noting that in S*EC v. Page Airways, Inc*., the defendant agreed to 'retain a Review Person to evaluate the methods and procedures followed in this investigation').

10 Amy Walsh, 'Is the Opaque World of Corporate Monitorships Becoming More Transparent?', Bus. L. Today (December 2015), https://www.americanbar.org/groups/business_law/publications/blt/2015/12/08_walsh/.

In the wake of – and likely to quell criticism over – that controversy, the DOJ first issued guidance on the retention and selection of monitors and has since updated its policies three times. The primary materials issued by the DOJ are as follows:

- *Morford Memorandum*: In March 2008, then acting Deputy Attorney General Craig Morford issued a memorandum establishing guidelines and decision-making procedures for the appointment of monitors titled 'Selection and Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations' (the Morford Memorandum).[11]
- *Breuer Memorandum*: In June 2009, Assistant Attorney General Lanny A Breuer issued a memorandum titled 'Selection of Monitors in Criminal Division Matters', in which he built on the Morford Memorandum, outlined the terms required in all monitorship agreements and refined the selection and documentation process for monitors.[12]
- *Grindler Memorandum*: Gary Grindler, then acting Deputy Attorney General, issued a memorandum in March 2010 titled 'Additional Guidance on the Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations' (the Grindler Memorandum), outlining the means by which corporations can reject a monitor's recommendation for being too costly. This guidance was the result of the increasing costs of monitorships and heavy public scepticism about their benefits.[13]
- *Benczkowski Memorandum*: In October 2018, Assistant Attorney General Brian A Benczkowski issued a memorandum titled 'Selection of Monitors in Criminal Division Matters' (the Benczkowski Memorandum) that supplemented the guidance provided by the Morford Memorandum. The Benczkowski Memorandum specifies, in greater detail, the principles for determining whether a monitor is needed and formalises in many ways the procedures for monitor nomination, selection and approval.[14]

As a result of these policies, the DOJ's selection process is arguably the most formalised and transparent of any agency. Nevertheless, concern over the selection and use of monitors abounds and the DOJ continues to internally assess the practice.[15] As a consequence of this escalating debate, the American Bar

11 Memorandum from Craig S Morford, Deputy Att'y Gen., to All Component Heads and US Att'ys, Selection and Use of Monitors in Deferred Prosecution Agreements (7 March 2008) (the Morford Memorandum).

12 Memorandum from Lanny A Breuer, Assistant Att'y Gen., to All Criminal Div. Personnel, Selection of Monitors in Criminal Division Matters (24 June 2009).

13 Memorandum from Gary G Grindler, Deputy Att'y Gen., Additional Guidance on the Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations (25 May 2010) (the Grindler Memorandum).

14 Memorandum From Brian A Benczkowski, Assistant Att'y Gen., Selection of Monitors in Criminal Division Matters (11 October 2018) (the Benczkowski Memorandum).

15 Rod Rosenstein, Deputy Att'y Gen., Keynote Address on Corporate Enforcement Policy (6 October 2017) ('We also will review the Department's practices concerning corporate monitors,

Association promulgated black-letter standards for monitors in August 2015 (ABA Standards).[16] The ABA Standards address a variety of issues, ranging from the selection and evaluation of monitors to the establishment of monitor work plans, and are 'the culmination of three years of work by an ABA task force in consultation with judges, prosecutors, defence counsel, court personnel, and academics'.[17]

Controversy over monitors has extended to the courtroom, as companies and monitors battle over, *inter alia*, the legality of court-appointed monitors and the scope of the monitor's powers,[18] the monitor selection process and the confidentiality of monitor reports.[19]

See Sections 32.4 and 32.5.5

United Kingdom 32.2.2

As the use of corporate monitors grew in the United States after the collapse of Enron, so UK authorities increasingly recognised the possibility of deploying similar monitorships as part of the resolution of their own corporate criminal investigations.[20] At the outset, this was done *ad hoc* and at the instigation of the relevant investigating authority. By way of example, in 2008 the Serious Fraud Office (SFO) settled civil proceedings against Balfour Beatty arising out of a construction project in Alexandria, Egypt. As part of that settlement, the SFO

---

the FCPA Pilot Program, corporate investigation training programs, and the mandate of the Financial Fraud Enforcement Task Force.'). See infra Section 32.3.

16 ABA Standards for Monitors (standards adopted August 2015).

17 Amy Walsh, 'Is the Opaque World of Corporate Monitorships Becoming More Transparent?', Bus. L. Today (December 2015), https://www.americanbar.org/groups/business_law/publications/blt/2015/12/08_walsh/. The ABA Standards provide a much more detailed discussion of best practices and considerations for the principles articulated in the DOJ guidance.

18 For example, after a district court in the Southern District of New York found that Apple violated the Sherman Antitrust Act, the court ordered that Apple be subject to a compliance monitor. Apple challenged the appointment both before the district court and, thereafter, the Second Circuit Court of Appeals, alleging, *inter alia*, that the appointment violated the constitutional separation of powers. See *United States v. Apple Inc.*, 787 F.3d 131, 136 (2d Cir. 2015). As but one example of the alleged constitutional violation, Apple highlighted that after it had moved the district court for a stay of the injunction appointing the monitor, the monitor 'coordinated with the plaintiffs . . . and submitted an affidavit as an integral part of the opposition papers.' Id. at 134, 138. The district court found that the monitor's actions did not evidence the monitor's prejudice against Apple, and though the Second Circuit concurred, it was far more critical of the monitor's conduct: 'It is certainly remarkable that an arm of the court would litigate on the side of a party in connection with an application to the court he serves.' The Second Circuit also noted that the monitor's submission on behalf of the plaintiffs 'was the opposite of best practice for a court-appointed monitor'. Id. at 138.

19 Marieke Breijer, 'ABA London: Keep monitor reports private', Global Investigations Review (13 October 2015), http://globalinvestigationsreview.com/article/1024106/aba-london-monitor-reports-private.

20 See further Jo Rickards and Johanna Walsh, 'DPA corporate monitorships in the UK', Global Investigations Review (21 September 2015), http://globalinvestigationsreview.com/article/1018143/dpa-corporate-monitorships-uk.

required the company to accede to 'a form of external monitoring for an agreed period'. This was an early example of the SFO fashioning new tools to remedy perceived corporate governance failings.

Another example was the SFO's successful prosecution of a construction firm, Mabey & Johnson Ltd, in 2009. This was the first-ever successful prosecution of a British company on charges of overseas corruption and breaching United Nations sanctions, and as part of its guilty plea Mabey & Johnson agreed to the appointment of an independent monitor for three years to oversee future conduct. Although this monitorship was approved by the court, Judge Geoffrey Rivlin QC[21] noted that it was likely to prove an expensive exercise and ordered that the costs of the monitor for the first year be capped at £250,000.

Nonetheless, the use of monitorships remained a novelty in the United Kingdom in the absence of a formal statutory footing. Indeed, it even drew notable judicial criticism on occasion. In the case of Innospec Ltd,[22] a manufacturer found to have paid substantial bribes to Indonesian officials, the English courts expressly criticised the three-year monitorship regime that had been jointly agreed by the SFO and DOJ as part of a 'global settlement' with the company. This was to be the first-ever US–UK joint monitorship, and illustrated the extent to which the UK investigating authorities were attracted by the US regime in adopting monitorships in the determination of corporate criminal investigations.

However, although the English court was prepared to approve this aspect of the settlement, the case – and in particular the terms of the cross-border determination reached between the parties – was controversial. Most unusually, a senior appellate judge, namely Lord Justice Thomas,[23] was brought in to sit on the case at first instance. He made clear that the court's approval for the appointment of a joint monitorship 'should be no precedent for the future'. In particular, he stated that the dual monitorship risked incurring unnecessary costs, and noted that 'imposing an expensive form of "probation order" seems to me unnecessary for a company which will also be audited by auditors well aware of the past conduct and whose directors will be well aware of the penal consequences of any similar criminal conduct.' In his view, the sums used on such monitoring might have been better allocated to paying fines or compensation. Either way, he made clear that in future 'the request for such an order will have to be fully explained in terms of its cost effectiveness.'[24]

Innospec was widely seen as a setback for bilateral appointment of monitorships and signalled some judicial resistance to the US approach to presenting the court with a sentencing or settlement package to be approved. But, in spite of Lord Justice Thomas's reservations, UK investigating authorities continued to seek and obtain orders for corporate monitorships, and these were included in

21 Later and on his retirement as a judge, he became s senior adviser to the Director of the Serious Fraud Office.

22 See *R v. Innospec Limited* [2010] Crim LR 665.

23 Lord Chief Justice of England and Wales 2013-2017.

24 *R v. Innospec Limited* [2010] Crim LR 665 at ss.48-49.

civil recovery orders agreed between the SFO and both Macmillan Publishers (in 2011) and Oxford Publishing[25] (in 2012). However, the actual and prospective role of monitorships as a tool of corporate compliance has increased substantially since the creation of the DPA regime in the United Kingdom, introduced by the Crime and Courts Act 2013. In light of that legislation, it is now clear that corporate monitorships have an express and permanent statutory place in the UK criminal law calendar of powers and remedies for holding a corporation to account.[26]

Following the passing of that Act, the SFO launched a consultation process in June 2013 to finalise a Code of Practice for the new DPA regime (the Code). The Code was issued on 14 February 2014, and gives close attention to the role and duties of corporate monitors. Although such monitorships are not a mandatory feature of the new regime, the focus on monitoring in the Code is a powerful indication of the role that UK authorities expect them to play in the future. The Code also sets out a detailed framework for the appointment of monitors, the costs and terms of the monitorship, and the areas that the monitor may be expected to supervise or restructure.[27]

The SFO's first application for a DPA was approved by a senior appellate judge, Sir Brian Leveson, then President of the Queen's Bench Division, on 30 November 2015.[28] The DPA involved Standard Bank Plc, which was the subject of bribery charges relating to multimillion-dollar payments made by a former sister company in Tanzania. As part of the agreed DPA, Standard Bank agreed to submit, at its own expense, to an 'independent review of its existing internal anti-bribery and corruption controls, policies and procedures regarding compliance with the Bribery Act 2010 and other applicable anti-corruption laws'.[29] The independent reviewer appointed was PricewaterhouseCoopers LLP. In his judgment approving the DPA, Leveson P made a number of observations about the difference between the DPA regimes in the United Kingdom and the United States, noting that '[i]n contra-distinction to the United States, a critical feature of the statutory scheme in the UK is the requirement that the court examine the proposed agreement in detail, decide whether the statutory conditions are satisfied and, if appropriate, approve the DPA.' In particular, he observed that the court will only approve a DPA if it is fair, reasonable and proportionate in all the circumstances, but that it will typically consider this question in private so as not

25 See the SFO's press release describing the circumstances of this settlement, which arose because of the publisher's unlawful practices in Kenya and Tanzania: https://www.sfo.gov.uk/2012/07/03/oxford-publishing-ltd-pay-almost-1-9-million-settlement-admitting-unlawful-conduct-east-african-operations/.

26 See Crime and Courts Act 2013, Schedule 17, Part I, s.5(3)(e).

27 See in particular s.7 of the DPA Code of Practice, headed 'Terms'.

28 See the SFO's press release: https://www.sfo.gov.uk/2015/11/30/sfo-agrees-first-uk-dpa-with-standard-bank/.

29 Id.

to prejudice any potential prosecution in the event of an adverse decision.[30] In the case of Standard Bank, he declared himself fully satisfied that the DPA was in the interests of justice.[31]

Following the high-profile *Standard Bank* case, the SFO soon made a second successful application for a DPA, approved by Leveson P on 6 July 2016.[32] The company, Sarclad Limited, which originally could not be named because of parallel legal proceedings, pleaded guilty to charges of conspiracy to corrupt. The DPA provided that Sarclad would undertake a review of its internal compliance controls, and that its chief compliance officer would prepare a report for submission to the SFO on its anti-corruption policies and their implementation, to be submitted within 12 months of the DPA and then annually for the DPA's duration.[33] Although it is not known why this approach was taken by the SFO, it seems likely that it was because the company in question was relatively small and the appointment of a full-time monitor would have been unduly financially onerous. Again, this would appear to demonstrate the flexibility with which UK authorities are now prepared to apply monitoring tools to fashion bespoke remedies for corporate wrongdoing.

Another example is the DPA agreed between the SFO and Tesco Stores Ltd, the supermarket conglomerate, on 28 March 2017 in respect of alleged accounting irregularities. Deloitte was appointed to a monitoring role to review and report on Tesco's controls and governance in respect of the recognition of commercial income.[34] This suggests an ever wider role for corporate monitorships in the United Kingdom, which may be imposed in contexts beyond international bribery and corruption. However, the touchstone for the appropriateness of a monitorship is always likely to be how the corporate has responded to allegations of wrongdoing: in the recent DPA agreed between the SFO and Serco Geografix Ltd,[35] dated 2 July and judicially approved on 4 July 2019, the SFO was satisfied that an undertaking of ongoing co-operation by its parent and a far-reaching corporate renewal programme were sufficient to make a monitorship unnecessary.

Nonetheless, the use of corporate monitorships looks set to increase in the United Kingdom, and a greater convergence with US practice can be expected. This is all the more so given the appointment of Lisa Osofsky, a former deputy general counsel of the FBI, as Director of the SFO in 2018. In a keynote speech on 17 October 2018, Ms Osofsky highlighted the differences between the UK

30 See *SFO v. Standard Bank Plc* [2016] Lloyd's Rep FC 102 at para. 2.

31 Id. at para. 22.

32 See the SFO's press release: https://www.sfo.gov.uk/2016/07/08/sfo-secures-second-dpa/.

33 See *SFO v. XYZ Ltd*, unreported, 24 June 2016 at para. 64.

34 See FCA Final Notice to Tesco Stores Ltd dated 28 March 2017, at s.4.10. The DPA was later approved by Leveson P at a hearing on 10 April 2017 and reporting restrictions were lifted in January 2019 following the acquittal of three individuals, https://www.sfo.gov.uk/2019/01/23/deferred-prosecution-agreement-between-the-sfo-and-tesco-published/.

35 See the DPA between Serco Geografix Ltd and the Serious Fraud Office, 2 July 2019, https://www.sfo.gov.uk/download/deferred-prosecution-agreement-serco-geografix-ltd-sfo/ at para. 5(ii)(b)(i) and (iii) and *Serious Fraud Office v. Serco Geografix Ltd* [2019] Lloyd's Rep FC 518.

and US regimes in respect of corporate prosecutions and DPAs but indicated that the SFO may take a more interventionist approach in future. Above all, she stressed that the SFO 'will want assurance that companies are doing everything they can to ensure the crimes of the past won't be repeated'.[36] In that context, and subject to the terms of the Code, the UK authorities' approach to the appointment and conduct of corporate monitors is ever more likely to follow the lead of the United States in the coming years.

See chapter 23 on negotiating global settlements

Circumstances requiring a monitor 32.3

In general, the DOJ assesses the need for the appointment of a monitor based on whether the corporation is capable of remediating, or has already remediated, its past wrongdoings without the assistance of a monitor. That, in turn, often translates into an enquiry of 'tone at the top' – whether, *inter alia*, management was involved in the criminal conduct, was negligent in failing to implement a proper compliance programme, fostered a culture that bred non-compliance with ethical and legal duties, and, critically, self-reported the misconduct to the DOJ.[37] The DOJ places significant weight on a company's decision to self-report, as evidenced by its treatment of monitors in the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy, announced on 29 November 2017,[38] and most recently updated in November 2019.[39] The Corporate Enforcement Policy states: 'When a company has voluntarily self-disclosed misconduct in an FCPA matter, fully cooperated, and timely and appropriately remediated . . . there will be a presumption that the company will receive a declination absent aggravating circumstances involving the seriousness of the offense or the nature of the offender.'[40] Further, '[i]f a criminal resolution is warranted', the DOJ 'generally will not require appointment of a monitor if a company has, at the time of resolution, implemented an effective compliance program.'[41] Significantly, the DOJ has recently signalled its intent to apply the Corporate Enforcement Policy's

See Chapters 3 and 4 on self-reporting to authorities

36 Keynote speech on Future SFO Enforcement at New York University School of Law (17 October 2018), https://wp.nyu.edu/compliance_enforcement/2018/10/16/director-of-the-serious-fraud-office-lisa-osofsky-keynote-on-future-sfo-enforcement/.

37 See 'Is a Corporate Monitor Necessary?', Corp. Crime Rep. (8 May 2013), www.corporatecrimereporter.com/news/200/isamonitornecessary05082013/.

38 Rod Rosenstein, Deputy Attorney General, Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (29 November 2017).

39 Justice Manual, US Dep't of Justice, § 9-47.120 (last updated November 2019).

40 Id.

41 Id.

See Chapters 3 and 4 on self-reporting to authorities

principles to other white-collar matters,[42] further emphasising the value it places on self-disclosure. Therefore, with increased self-reporting, it is reasonable to expect that monitorships will decline.[43]

In addition to self-reporting, the Morford Memorandum sets forth two broad considerations to guide prosecutors when deciding when a monitor is appropriate: '(1) the potential benefits that employing a monitor may have for the corporation and the public, and (2) the cost of a monitor and its impact on the operations of a corporation.'[44] Because of the breadth of these considerations, the DOJ, through the Benczkowski Memorandum, offered further guidance, and in particular clarified that when assessing 'potential benefits' of the monitorship, one must consider, among other factors: (1) if the misconduct involved the manipulation of books and records or the exploitation of an inadequate compliance programme, (2) the pervasiveness of the misconduct across the business organisation and the degree of its facilitation by senior management, (3) investments by the corporation to improve its compliance programme and internal controls, and (4) whether these remedial improvements had been tested to detect or prevent future similar misconduct.[45] These considerations must be weighed in light of case-specific factors, including the particular regions and industries involved.[46]

Notably, the Benczkowski Memorandum also states that the Criminal Division of the DOJ should only favour the imposition of a monitor when there is a 'demonstrated need for, and a clear benefit' from the monitorship relative to the 'projected costs and burdens' it will create.[47] The defence bar read this as a marked shift away from monitorships. Benczkowski corrected this misimpression

42 Kelly Swanson, 'DOJ expanding use of FCPA declination policy principles', Global Investigations Review (2 March 2018), https://globalinvestigationsreview.com/article/1166274/doj-expanding-use-of-fcpa-declination-policy-principles.

43 Deputy Attorney General Sally Quillian Yates's September 2015 memorandum, 'Individual Accountability for Corporate Wrongdoing' (the Yates Memorandum), reinforces the importance of internal risk assessment and compliance monitoring. As promulgated, the Yates Memorandum requires early and complete self-reporting if a corporation wishes to obtain co-operation credit. Corporations are thus highly incentivised to self-report.

44 Morford Memorandum, supra note 11, at 2.

45 Benczkowski Memorandum, supra note 14, at 2.

46 Commentators have noted that monitorships may be appropriate where companies have faced significant cybersecurity breaches, such as Yahoo!, where a recent breach resulted in the theft of data from more than one billion accounts. See Jacob S Frenkel and Justin L Root, 'Analysis: Cyber-Monitoring: The Next Frontier' (7 March 2017), http://www.dickinson-wright.com/-/media/files/news/2017/03/analysis-cyber-monitoring-the-next-frontier.pdf?la=en. In such cases, the severity of the breach and the complexity of the problem are two factors that may well have a bearing on a decision to impose a monitor.

47 Benczkowski Memorandum, supra note 14, at 2. See also Deputy Assistant Att'y Gen. Matthew S Miner Remarks at the 29th Annual National Institute on Health Care Fraud, New Orleans, 9 May 2019, available at https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-gives-remarks-29th-annual-national (noting the 'bottom line' is that the 'Criminal Division should favor the imposition of a monitor only where there is a demonstrated need for, and clear benefit to be derived from, a monitorship relative to the projected costs and burdens').

in a keynote address in April 2019: 'Put simply, this guidance was not meant to do away with monitors – it was meant to focus our prosecutors' determination on the appropriate factors so that monitors are imposed only where necessary and under the terms and scope that is appropriate for that given case.'[48] In the wake of this guidance, the DOJ has seemingly tailored monitorships more narrowly to the issues at hand, as demonstrated by Walmart's recent settlement, discussed further below. The DOJ also seems willing to adopt quasi-monitorship structures, where a full-blown monitorship is ill-suited.[49]

Note that even corporations registered under the laws of a foreign country are subject to DOJ monitorships, provided the United States has jurisdiction over the corporation's misconduct. Indeed, in recent years in the United States, monitors have been imposed on foreign offenders with increased frequency.[50]

48 Assistant Att'y Gen. Brian A Benczkowski Keynote Address at the Ethics and Compliance Initiative 2019 Annual Impact Conference, Dallas, Texas, 30 April 2019, https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-keynote-address-ethics-and; see also Adam Dobrik, 'Criminal division chief plays down talk of monitorship demise', Global Investigations Review (8 March 2019), available at https://globalinvestigationsreview.com/article/jac/1181316/criminal-division-chief-plays-down-talk-of-monitorship-demise (quoting Benczkowski, 'There were many who thought [the Benczkowski Memorandum] reflected a sort of Shakespearean policy of first, let's kill all the monitors. But that's not what it was meant to do . . . . In fact, it was meant to provide greater clarity both to companies but also to our prosecutors to ensure that when they do recommend the appointment of a monitor that they are doing so for the right reasons and with the right scope.').

49 In July 2019, Facebook entered into a record-breaking $5 billion settlement with the Federal Trade Commission (FTC) and DOJ over data privacy claims. The consent order requires Facebook to appoint an 'independent assessor', chosen by Facebook but approved by the FTC and DOJ, to monitor its compliance with the terms of the order for a 20-year term. Plaintiff's Consent Motion for Entry of Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief and Memorandum in Support at 5, *United States v. Facebook, Inc.*, No. 19-cv-02184 (D.D.C. 24 July 2019); Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief at 4, *United States v. Facebook, Inc.*, No. 19-cv-02184 (D.D.C. 24 July 2019). The independent assessor must, *inter alia*, conduct an initial and biennial assessment of Facebook's privacy programme, to be shared with the FTC and DOJ, and attend quarterly meetings with a newly established independent privacy committee of the board of directors, both with and without management present, to discuss privacy risks. Decision and Order at VIII.F, X.A.5, *In re Facebook, Inc.*, Docket No. C-4365 (F.T.C. 24 July 2019).

50 See SEC press release, 'VimpelCom to Pay $795 Million in Global Settlement for FCPA Violations' (18 February 2016), https://www.sec.gov/news/pressrelease/2016-34.html (noting that the SEC imposed a monitor on Dutch company VimpelCom as part of the parties' settlement to resolve VimpelCom's FCPA violations); Independent Monitor of Takata and the Coordinated Remedy Program, Takata Monitor, www.takatamonitor.org/ (Japanese company Takata agreeing to a monitor in connection with its settlement with the US National Highway Traffic Safety Administration for Takata's manufacture and sale of ammonium nitrate airbags).

Similar tests are applied in the United Kingdom. The Code sets out some important considerations for the appointment of a monitor, including whether the company already has a 'genuinely proactive and effective corporate compliance programme', and whether the appointment would be fair, reasonable and proportionate in all the circumstances.[51]

As in the United States, there is likely to be a particular focus on the degree of culpability of the management, especially if that management is still in place. Where the management has been entirely replaced, or where misconduct has been self-reported, there may be less need for an extended monitorship (see, for example, the observations made by the court in *Innospec*).[52] Moreover, and again in light of the comments in *Innospec*, the United Kingdom is likely to apply a special focus to matters of cost-effectiveness. Much is likely to turn on an analysis of what is fair, reasonable and proportionate in the circumstances of the specific proposed monitorship.

32.4 Selecting a monitor

The selection of the monitor is often the most controversial aspect of monitorships, as claims of cronyism abound. As outlined by the Morford Memorandum, the government should ensure that the monitor is highly qualified, does not have any conflict of interests (either with the government or the corporation), and will instil public confidence in the monitorship process.[53] The Benczkowski Memorandum attempts to standardise the selection process by creating a Standing Committee on the Selection of Monitors (the Standing Committee).[54] The Standing Committee comprises (1) the Deputy Assistant Attorney General with supervisory responsibility for the Fraud Section, who also serves as the chair of the Standing Committee, (2) the Chief of the Fraud Section (or other relevant Section), and (3) the Deputy Designated Agency Ethics Official for the Criminal Division.[55] To the extent any of these individuals are unable to serve, they may designate a replacement. To the extent further replacements are necessary for any given case, the chair of the Standing Committee may appoint them.[56]

The ABA Standards suggest that both parties 'have a significant role in the selection process', enumerate multiple selection criteria, and outline mandatory and potential exclusions.[57] To this end, the Benczkowski Memorandum provides for the corporation to recommend three qualified candidates through a written proposal. The proposal should provide a description of the candidates' qualifications and credentials; certification that the candidates have no current or future affiliation with the corporation and no conflict of interest in serving as the monitor;

51 See in particular s.7.11 of the DPA Code of Practice.

52 *R v. Innospec Limited* [2010] Crim LR 665 at ss.48-49.

53 Morford Memorandum, supra note 11, at 3.

54 Benczkowski Memorandum, supra note 14, at 5.

55 Id. at 3-4.

56 Id. at 3.

57 ABA Standards for Monitors §§ 24–2.1; 24–2.4.; 24–2.4(3)–(4).

and a statement identifying the corporation's first choice to serve as monitor.[58] The Criminal Division attorneys handling the matter and their supervisors assess the candidates according to the factors detailed in the Benczkowski Memorandum, and recommend one of the candidates to the Standing Committee.[59] The Standing Committee votes on the recommended candidate and forwards their acceptance or rejection to the Assistant Attorney General of the Criminal Division, who must review and consider the recommendation (and cannot unilaterally accept or veto it).[60] As a further layer of review, all monitor candidates selected pursuant to DPAs, NPAs and plea agreements must be approved by the Office of the Deputy Attorney General.[61]

One issue with past selection methods is that they have not resulted in a diverse monitor pool.[62] For example, between 2004 and 2018, only three women and three non-white attorneys (all male) have been chosen by the DOJ to serve as FCPA monitors, even though there have been more than 45 settlements involving FCPA monitors during the same period.[63] The DOJ appears to be alive to this issue. On 30 April 2018, the DOJ and a US-based subsidiary of Panasonic entered into a DPA to resolve FCPA violations, under which the company agreed to a two-year monitorship.[64] The DOJ included a provision in the DPA that stated: 'Monitor selections shall be made in keeping with the Department's commitment to diversity and inclusion.'[65] The DPA also includes various provisions that enable the DOJ to broaden the group of candidates from which it will select the monitor.[66] While the DOJ cannot consider non-merit-based factors such as race and gender when choosing the most-qualified candidate, these provisions help

58 Benczkowski Memorandum, supra note 14, at 5.

59 Id. at 5-7. Factors for consideration include the candidates' credentials, experience and expertise, degree of objectivity and independence from the corporation, adequacy of resources to discharge responsibilities and any other relevant factors, as determined by the reviewing attorneys.

60 Id. at 7-8.

61 Id. at 8.

62 Dylan Tokar, 'Women and minorities lose out in FCPA monitor selection process', Global Investigations Review (1 February 2018), https://globalinvestigationsreview.com/article/jac/1153265/women-and-minorities-lose-out-in-fcpa-monitor-selection-process.

63 Id. These statistics were made available after a court battle fought by a Global Investigations Review reporter. The reporter filed a lawsuit in December 2016, seeking the names of monitor candidates considered for 15 companies involved in compliance investigations, and the names of the DOJ attorneys involved in the selection process. In March 2018 he prevailed, when the District Court for the District of Columbia ruled that the public's interest in learning the candidates' identities outweighed the government's privacy interest. See *Tokar v. U.S. Dep't of Justice*, No. 16-2410, 2018 WL 1542320 (D.D.C. 29 March 2018); Jody Godoy, 'DOJ Sued by Reporter Seeking FCPA Monitor Records', *Law 360* (9 December 2016), https://www.law360.com/articles/871052/doj-sued-by-reporter-seeking-fcpa-monitor-records.

64 Dep't of Justice Deferred Prosecution Agreement with Panasonic Avionics Corp., 30 April 2018, available at https://www.justice.gov/opa/press-release/file/1058466/download.

65 Id. at 12.

66 Id. ('If the Fraud Section determines, in its sole discretion, that any of the candidates are not, in fact, qualified to serve as the Monitor, or if the Fraud Section, in its sole discretion, is not satisfied with the candidates proposed, the Fraud Section reserves the right to request that the company

ensure that the pool from which the DOJ makes its selection is more diverse. A DOJ spokesperson indicated that the above quoted language was added to the Criminal Division's standard agreements last year,[67] and therefore it will likely be a recurring feature in the department's DPAs. It also remains to be seen whether the protocols established by the Benczkowski Memorandum will help create a more diverse monitor pool.

There is also an open question as to judicial oversight of the selection process. In March 2017, the DOJ reached a plea agreement with ZTE for conspiring to violate export control laws, under which ZTE would be subject to a three-year monitorship, with the monitor selected by the DOJ 'in its sole discretion' out of a pool of candidates proposed by ZTE.[68] In an unprecedented move, the court overseeing the matter – the District Court for the Northern District of Texas – amended the terms of the plea agreement to impose a monitor of its own selection and to increase judicial oversight over the monitorship.[69] Specifically, the plea agreement was amended to state that James M Stanton would be appointed as ZTE's monitor,[70] that 'the Monitor is a *judicial adjunct* pursuant to Federal Rule of Civil Procedure 53'[71] and that '[a]ll reports, submissions, or other materials encompassed by this agreement will be filed [with the Court].'[72] The appointment of Mr Stanton, a lawyer in private practice and a former Texas state judge, is seen by some as particularly unusual given his lack of monitorship experience.[73]

---

nominate additional candidates. In the event the Fraud Section rejects any proposed monitors, the Company shall propose additional candidates . . . so that three qualified candidates are proposed.').

67 Clara Hudson, 'Lawyers laud criminal division's diversity provision for monitors', Global Investigations Review (3 May 2018), https://globalinvestigationsreview.com/article/jac/1168991/lawyers-laud-criminal-divisions-diversity-provision-for-monitors.

68 Plea Agreement at Attachment A ¶¶ 1–2, *United States v. ZTE Corp.*, No. 17-0120-K (N.D. Tex. 7 March 2017) ('[T]he Company will propose to the Department three candidates to serve as the Monitor. . . . The Department retains the right, in its sole discretion, to accept or reject the Monitor candidates proposed by the Company.').

69 The process for selecting the monitor and the terms of the monitorship were outlined in Attachment A to the Plea Agreement. The court subsequently amended Attachment A but left the remainder of the Plea Agreement intact. See Attachment A (Modified) Independent Corporate Compliance Monitor, *United States v. ZTE Corp.*, No. 17-0120-K (N.D. Tex. 22 March 2017). See also Rearraignment Hearing, *United States v. ZTE Corp.*, No. 17-0120-K (N.D. Tex. 22 March 2017) ('Here's what the agreement is as I understand it: It would be a sentence of three years probation on each count, to run concurrently, with an independent corporate compliance monitor appointed by me, by the Court, which is – I have chosen Mr. James Stanton; or if something happens to him or if I choose to change, that would be who it would be, as set out in Attachment A as modified today.').

70 Attachment A (Modified) Independent Corporate Compliance Monitor ¶ 1, *United States v. ZTE Corp.*, No. 17-0120-K (N.D. Tex. 22 March 2017) ('ZTE Corporation . . . agrees to engage James M. Stanton as an independent corporate monitor . . . .').

71 Id. ¶ 6 (emphasis added).

72 Id. ¶ 13.

73 See Sue Reisinger, 'In Rare Move, Judge Imposes Own Monitor in ZTE Plea Deal', The American Lawyer (29 March 2017), http://www.americanlawyer.com/id=1202782436926/In-Rare-Move-Judge-Imposes-Own-Monitor-in-ZTE-Plea-Deal?mcode=0&curindex=0&curpage=ALL (noting that James Stanton is a civil and personal injury lawyer with no prior experience of acting as a

Notably, ZTE's monitorship was imposed as part of a plea agreement, which the court must review and approve. Accordingly, the court had the opportunity to amend the terms of the agreement before approving the plea. It remains to be seen whether courts will take as active a role in crafting the terms of monitorships imposed as part of DPAs and NPAs, which do not require the court's approval.[74]

In the United Kingdom, a slightly different appointment procedure has been laid down by the Code. As part of the negotiations surrounding a DPA in the United Kingdom, the company must provide the prosecuting authority and the court with details of three potential monitors, including their qualifications, their estimated costs and any links with the relevant company. The company should then indicate their preferred monitor of the three, stating the reasons for their preference. This choice will ordinarily be accepted by the prosecuting authority and court, except where a conflict of interest or a lack of relevant experience has been identified.[75]

In terms of eligibility, the monitor must be independent from the company, and thus former employees, clients and close acquaintances are likely ineligible. Additionally, as the requirements of the monitorship will differ case by case, the monitor should be selected based on how well his or her qualifications pair with the requirements of the relevant monitorship.[76] For example, the DPA between the DOJ and Panasonic lists the minimum contemplated qualifications of a monitor as (1) 'sufficient independence' from Panasonic, (2) 'demonstrated expertise with respect to the FCPA and other applicable anti-corruption laws, including experience counseling on FCPA issues', (3) 'experience designing and/or reviewing corporate compliance policies, procedures and internal controls, including FCPA and anti-corruption policies, procedures, and internal controls', and (4) 'ability to access and deploy resources necessary to discharge the Monitor's duties' under the agreement.[77]

In global settlements, both US and UK authorities increasingly see the value of appointing a monitor experienced in the laws of the relevant jurisdiction.[78] Although the Morford Memorandum suggests that non-attorney experts 'such as accountants, technical or scientific experts, and compliance experts' may be better qualified for certain monitorships, in practice, in both the US and UK monitors are predominantly lawyers, and often have prosecutorial experience.[79]

---

monitor and no significant criminal experience, albeit per his resume he has served as a special master and arbitrator in six civil cases).

74 See *United States v. Fokker Services BV*, 818 F.3d 733, 741 (D.C. Cir. 2016).

75 See in particular ss.7.15-7.17 of the DPA Code of Practice.

76 See Benczkowski Memorandum, supra note 14, at 2.

77 Dep't of Justice Deferred Prosecution Agreement with Panasonic Avionics Corp. at 11-12, 30 April 2018, available at https://www.justice.gov/opa/press-release/file/1058466/download.

78 See infra notes 102-104 and accompanying text discussing Rolls-Royce's monitor, British lawyer Lord Gold.

79 One study found that half of all monitors appointed in connection with DPAs and NPAs since 2001 have been former prosecutors, leading some critics to describe the monitoring industry as a 'full employment act for former federal prosecutors'. See Alison Frankel, 'DOJ should end secret

Note, however, as the requirements of the monitorship can evolve over the duration of the monitorship, and the appointed monitor may prove to be incompatible with the corporation, the government may replace the monitor and the monitor is free to resign. As one example of a rather tumultuous monitorship, Western Union went through four monitors as part of a 2010 settlement for failing to comply with anti-money laundering laws.[80]

To avoid such situations, third-party organisations have devoted themselves to promoting the use, quality and efficiency of monitors.[81] For example, the International Association of Independent Corporate Monitors – whose board is itself composed of many former monitors – offers resources and training to professionals, and has established a Code of Professional Conduct to serve as a template for best standards and practices.[82]

32.5 The role of the monitor

32.5.1 Scope of the monitorship

The scope of the monitorship should be tailored to the circumstances of each case, with the ultimate goal of reducing the risk of recurrence of the corporation's misconduct.[83] Therefore, the monitor's role should normally include a mandate for oversight, review and proposed modification of a company's compliance programme to facilitate rehabilitation of existing misconduct and deterrence of future

selection process for corporate watchdogs', Reuters Blog (14 July 2014), http://blogs.reuters.com/alison-frankel/2014/07/14/doj-should-end-secret-selection-process-for-corporate-watchdogs/; Steven Davidoff Solomon, 'In Corporate Monitor, a Well-Paying Job But Unknown Results', *The NY Times: Dealbook* (15 April 2014), http://dealbook.nytimes.com/2014/04/15/in-corporate-monitor-a-well-paying-job-but-unknown-results/. As but one recent example, the former Deputy Chief in the Fraud Section of the Criminal Division of the DOJ was recently appointed to serve as a monitor for Odebrecht as part of its guilty plea for FCPA violations. See Jody Godoy, 'DOJ Taking $24m Haircut on Odebrecht's $2.6B FCPA Fine', *Law 360* (12 April 2017), https://www.law360.com/articles/912549/doj-taking-24m-haircut-on-odebrecht-s-2-6b-fcpa-fine; Biography of Charles E. Duross, Morrison Foerster, https://www.mofo.com/people/charles-duross.html.

80 Rachel Louise Ensign and Max Colchester, 'Meet the Private Watchdogs Who Police Financial Institutions', *The Wall Street J.* (30 August 2015), www.wsj.com/articles/meet-the-private-watchdogs-who-police-financial-institutions-1440983917. On 9 June 2017, a court accepted the monitor's final report, thereby ending Western Union's monitorship. See The Western Union Company, Form 8-K, filed 9 June 2017.

81 International Association of Independent Corporate Monitors, 'About Us', at http://iaicm.org/about-independent-corporate-monitors/ (describing the mission/purpose of the organisation and discussing the Code of Professional Conduct) (last accessed 5 June 2017).

82 Id. (touting its members as having the 'breadth and depth of relevant skills, knowledge, and experience, together with reputation of character, to effectively serve as [monitors]'). See also Thomas Fox, 'IAICM Shine a Light on Corporate Monitors', JD Supra, 8 March 2017 http://www.jdsupra.com/legalnews/iaicm-shine-a-light-on-corporate-85994/. Membership is comprised of a 'distinguished panel of current and former corporate monitors, retired judges, and one former FBI agent'.

83 Morford Memorandum, supra note 11, at 5.

wrongdoing.[84] Accordingly, the monitor may be required to assist with structural changes, as well as help alter corporate culture and normative expectations.[85] In the United Kingdom, a list of items and procedures that the monitor may wish to consider as part of its monitoring programme is set out in the Code.[86]

Following the Benczkowski Memorandum, appropriate tailoring has become increasingly important and gives parties the opportunity to think carefully about the shape the monitorship should take.[87] In Walmart's June 2019 settlement with the DOJ over FCPA violations, the company agreed to a monitorship whose mandate was narrowed both by geography (to four countries and the company's headquarters) and subject matter (to specified Key Risk Areas).[88] The agreement specifically stated: 'The Monitor shall not conduct a comprehensive review of all business lines, all business activities, or all countries.'[89]

The monitor is an independent third party and does not serve as an employee or agent of either the corporation or the government.[90] Likewise, the monitor does not have an attorney–client relationship with either the corporation or the government. Nonetheless, it is critical for the monitor to have an open dialogue with, and co-operation from, the corporation and the government throughout the duration of the monitorship, which may include 'iterative work plans, planning

84 See for example Dep't of Justice Deferred Prosecution Agreement with Avon Products, Inc., 15 December 2014, available at https://www.sec.gov/Archives/edgar/data/8868/000000886814000073/exhibit992dpa.htm ('[T]he Monitor will evaluate, in the manner set forth below, the effectiveness of the internal accounting controls, record-keeping, and financial reporting policies and procedures of the Company as they relate to the Company's current and ongoing compliance with the FCPA . . . .').

85 Critics complain that '[l]ittle is publicly disclosed about what specifically they are supposed to accomplish [and] what they discover in their examinations.' Rachel Louise Ensign and Max Colchester, 'Meet the Private Watchdogs Who Police Financial Institutions', *The Wall Street J.* (30 August 2015), www.wsj.com/articles/meet-the-private-watchdogs-who-police-financial-institutions-1440983917.

86 See in particular s.7.21 of the DPA Code of Practice.

87 See, supra notes 46 and 47 and accompanying text.

88 Dep't of Justice Non-Prosecution Agreement with Walmart, Inc., Attachment C at ¶ 2, 20 June 2019, available at https://www.justice.gov/opa/press-release/file/1175791/download. The monitor's mandate was limited to an assessment of the 'Key Risk Areas', defined as 'anti-corruption-related internal auditing controls related to anti-corruption, record-keeping, and financial reporting policies and procedures of the Company as they relate to permits and licensing, real estate development and construction . . . donations . . . and third-party intermediaries', with several explicit carve-outs. The monitor's mandate was further limited to four countries, as well as Walmart's headquarters in Arkansas. Id.

89 Id. at ¶ 8.

90 Notably, some corporations have taken to hiring their own internal monitors following the government's implementation of a monitor. For example, as part of Western Union's 2010 settlement, Western Union received a monitor. Independently, Western Union also hired a consultant, leading to what in effect was a 'dual system of internal monitors – one stipulated by the settlement and the other hired by the money-transfer firm'. Rachel Louise Ensign and Max Colchester, 'Meet the Private Watchdogs Who Police Financial Institutions', *The Wall Street J.* (30 August 2015), www.wsj.com/articles/meet-the-private-watchdogs-who-police-financial-institutions-1440983917.

meetings prior to any substantive work, and mid-review meetings'.[91] The parties should also stipulate what, if any, role the government or court should play in resolving disputes that may arise between the monitor and the corporation.[92]

Though the monitor does not take on a prosecutorial function, he or she may nonetheless uncover continuing or undisclosed misconduct. The monitorship agreement 'should clearly identify any types of previously undisclosed or new misconduct that the monitor will be required to report directly to the [government]'. And, on the other hand, the agreement should identify any misconduct that the monitor can, in its discretion, report to the government, the corporation or both.[93]

32.5.2 Duration of the monitorship

Monitorships can range from months to several years. The duration of the monitorship will in large part depend on the scope of the monitorship, and in particular the extent of the problems found and the necessary remedial measures.[94] When negotiating duration, the parties should be mindful of, *inter alia*, the 'nature and seriousness of the underlying misconduct'; the 'pervasiveness and duration of the misconduct'; the complicity of senior management; the 'corporation's history of similar misconduct'; the corporate culture; the 'scale and complexity of any remedial measures contemplated by the agreement, including the size of the entity or business unit at issue'; and the current 'stage of design and implementation of remedial measures'.[95]

In most cases, the monitorship agreement will permit the government to extend the monitorship at its discretion if the corporation has not satisfied its obligations under the settlement, and provide for early termination if the corporation can demonstrate 'a change in circumstances sufficient to eliminate the need for a monitor'.[96] For example, after Credit Suisse admitted to aiding US tax evasion, the New York State Department of Financial Services appointed a monitor for what

91 F Joseph Warin, Michael S Diamant and Veronica S Root, 'Somebody's Watching Me: FCPA Monitorships and How They Can Work Better', 13 U. Pa. J. Bus. L. 321, 364 (2011), available at http://scholarship.law.upenn.edu/jbl/vol13/iss2/1.

92 Grindler Memorandum, supra note 13, § II.

93 Morford Memorandum, supra note 11, at 7. Critically, undisclosed or continuing misconduct may invalidate the terms of the settlement and lead to an extension of the term and scope of the monitorship.

94 Morford Memorandum, supra note 11, at 7-8.

95 Id. at 7. See Assistant Att'y Gen. Brian A Benczkowski Keynote Address at the Ethics and Compliance Initiative 2019 Annual Impact Conference, Dallas, Texas, 30 April 2019, available at https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-keynote-address-ethics-and (noting that a monitorship limited to two years was appropriate as part of Fresenius Medical Care's FCPA settlement, because the company 'had made a number of improvements to its compliance program but had not yet fully tested that program').

96 Morford Memorandum, supra note 11, at 8 ('For example, if a corporation ceased operations in the area that was the subject of the agreement, a monitor may no longer be necessary. Similarly, if a corporation is purchased by or merges with another entity that has an effective ethics and compliance program, it may be prudent to terminate a monitorship.').

was anticipated to be a two-year monitorship. However, shortly after the monitorship began in October 2014, a tolling period was triggered because Credit Suisse could not produce information at the pace and volume required by the monitor.[97] After more than three years of monitorship, the Department of Financial Services entered a consent order requiring Credit Suisse to engage an independent consultant for an additional year.[98] In the United Kingdom, this ability to extend monitorships has been formally recognised in the Code, subject to the extended term of the monitorship not exceeding the length of the DPA itself.[99]

Hybrid monitorships – in which the monitor serves for approximately 18 months and the corporation self-reports for the following 18 months – are also becoming increasingly common, especially in the context of FCPA investigations.[100] As a further nuance, the DOJ has, in some instances, agreed to defer to a pre-existing monitorship in lieu of establishing its own monitorship. As one example, the December 2015 settlement between Alstom and the DOJ, over Alstom's various FCPA violations, required that Alstom be subject to an independent monitor. However, Alstom was already subject to a monitor in connection with a 2012 settlement with the World Bank. Rather than implement a second monitor, the DOJ agreed to defer to the existing World Bank-appointed monitor, provided that, *inter alia*, Alstom self-report to the DOJ 'at no less than twelve-month intervals during a three-year term'.[101]

Rolls-Royce reached a similar resolution in its January 2017 settlement with US, UK and Brazilian authorities over bribery and corruption charges (and, in the United States, FCPA charges). At the time, Rolls-Royce already had an independent monitor – Lord Gold – who was appointed to review the company's anti-bribery and corruption compliance in connection with a 2013 settlement with the SFO. Though the company's 2017 DPA with the SFO did not impose a second monitor, it did require Rolls-Royce, *inter alia*, to procure a further report from Lord Gold outlining recommendations for change and produce a

97 John Letzing, 'Credit Suisse's Tardiness Likely to Extend Monitor's Sojourn', *The Wall Street J.* (6 January 2016), www.wsj.com/articles/credit-suisses-tardiness-likely-to-extend-monitors-sojourn-1452084986.

98 N.Y. Dep't of Fin. Services Consent Order, *In the Matter of Credit Suisse AG* (13 November 2017), available at https://www.dfs.ny.gov/docs/about/ea/ea171113.pdf.

99 See s.7.19 of the DPA Code of Practice.

100 FCPA Digest, 'Recent Trends and Patterns in the Enforcement of the Foreign Corrupt Practices Act' at 2, 6, Shearman & Sterling (6 January 2014), available at www.shearman.com/~/media/Files/Services/FCPA/2014/FCPADigestTPFCPA010614.pdf. For example, the DOJ's DPA with Panasonic requires a two-year monitorship, after which Panasonic is required to undertake follow-up reviews for the remainder of the agreement. Dep't of Justice Deferred Prosecution Agreement with Panasonic Avionics Corp. at 12–13, 30 April 2018, available at https://www.justice.gov/opa/press-release/file/1058466/download.

101 Dylan Tokar, 'With Alstom Monitor Agreement, DOJ Tries Something New', Global Investigations Review (4 February 2015), available at http://globalinvestigationsreview.com/article/1023537/with-alstom -monitor-agreement-doj-tries-something-new.

written plan of how it would implement these recommendations.[102] Likewise, the company's DPA with the DOJ did not implement a further monitor, but did require the company to report to the DOJ at least once a year for the next three years and to produce a series of reports.[103] When the SFO applied to the English Court for approval of the DPA, the senior judge who heard that application, Sir Brian Leveson, President of the Queen's Bench Division, expressly referred to the appointment of Lord Gold and the ongoing monitoring process as important factors indicating that Rolls-Royce had properly addressed issues of corporate compliance; this made the DPA (as opposed to criminal prosecution) an appropriate outcome.[104]

The 2019 *Serco Geografix* DPA took into consideration the fact that the parent company, Serco Group, had adopted an ongoing corporate renewal programme in 2013, which had been approved by the UK government, to improve assurance mechanisms and working practices within all companies in the group. In the approved judgment, Davis J said that this amounted to a significant remedial measure.[105]

32.5.3 Creating a work plan

Under the ABA Standards, the monitor should draft a detailed work plan at the outset of the monitorship, with input from the corporation and government.[106] This is also a requirement of the UK regime under the Code, which stipulates that a work plan should be prepared even before the monitor's appointment is finally approved.[107] The work plan will ordinarily include an overview of the monitor's role and objectives, a description of the corporation's policies and procedures to be evaluated, a list of documents the monitor seeks to review, and a list of persons the monitor seeks to interview. The work plan should also include a proposed timeline for reaching certain milestones, such as a review of documents concerning the corporation's compliance programme; interviews with senior management, the board of directors and audit committee; and deadlines for reporting of the

102 Deferred Prosecution Agreement between the SFO and Rolls-Royce, paras. 25 to 34, available at http://iaicm.org/wp-content/uploads/formidable/9/Rolls-Royce-SFO-DPA-17Jan2017.pdf.

103 Deferred Prosecution Agreement at 4–5, D-1, *United States v. Rolls-Royce PLC*, No. 16-0247 (S) (S.D. Ohio 20 December 2016) ('Based on the Company's remediation and the state of its compliance program, and the Company's agreement to report to the Fraud Section and the Office as set forth in Attachment D to this Agreement, the Fraud Section and the Office determined that an independent compliance monitor was unnecessary[.]').

104 *Serious Fraud Office v. Rolls-Royce Plc* [2017] Lloyd's Rep FC 249 at paras. 43-47 and 61-64.

105 *Serious Fraud Office v. Serco Geografix Limited* [2019] Lloyd's Rep FC 518 at para. 25.

106 If disclosing the work plan to the company would limit the monitor's effectiveness, however, the parties should consider an alternative arrangement. See ABA Standards for Monitors § 24-3.3(3).

107 See s.7.18 of the DPA Code of Practice.

monitor's findings.[108] In the United Kingdom, the work plan is required to set out provisions for costs and even to state with what frequency the monitor intends to report to the prosecutor.[109]

Not only does a detailed work plan help control costs and increase transparency, but it also helps prepare all parties for the monitorship.[110] Accordingly, the corporation will have a better understanding of what can be expected, and the act of preparing the work plan helps the monitor become familiar with the company's culture and risk tolerance. Further, a detailed work plan helps ensure that the monitor's expectations for the corporation are reasonable and that the government is comfortable with the monitor's approach.[111]

Reviewing documents and interviewing witnesses 32.5.4

To serve as an effective monitor and issue tailored recommendations to the corporation, the monitor must understand the corporation and its business. To develop this understanding, the monitor must have wide access to the documents and information deemed reasonably necessary to carry out the monitorship.[112] A recurring problem, however, is that given the monitor's independence, corporations are hesitant to disclose sensitive information. Under the ABA Standards, the corporation is not required to provide documents covered by the attorney–client or work-product privilege, or documents for which disclosure would be 'inconsistent with applicable law'.[113] A similar approach is adopted under the UK Code, which requires the company to grant the monitor 'complete access to all relevant aspects of its business during the course of the monitoring period', but does not affect the company's right to assert legal professional privilege over relevant documents.[114]

See Chapters 35 and 36 on privilege

108 Jason T Wright, 'The Corporate Compliance Monitor's Role in Regulatory Settlement Agreements', SRR (Spring 2014), www.srr.com/article/corporate-compliance-monitors-role-regulatory-settlement-agreements.

109 See s.7.18 of the DPA Code of Practice.

110 See Warin, supra note 91, at 360 (noting that the work plan also serves as a 'gloss on the settlement agreement to be applied in subsequent years of the monitorship').

111 Jason T Wright, 'The Corporate Compliance Monitor's Role in Regulatory Settlement Agreements', SRR (Spring 2014), www.srr.com/article/corporate-compliance-monitors-role-regulatory-settlement-agreements.

112 See Rachel Louise Ensign and Max Colchester, 'Meet the Private Watchdogs Who Police Financial Institutions', *The Wall Street J.* (30 August 2015), www.wsj.com/articles/meet-the-private-watchdogs-who-police-financial-institutions-1440983917 (noting that the monitorship involved over 3,500 meetings with HSBC staffers, 11,500 document requests, and over 2 million pages of documents).

113 ABA Standards for Monitors § 24-4.2(1)(a)–(2)(a). Despite the monitor's independence, the monitor still has a duty to the corporation by nature of the appointment. Thus, the monitor cannot use proprietary or confidential information obtained during the monitorship for any purpose other than in furtherance of the monitorship. Where proprietary information is disclosed, the monitor and corporation should work together to ensure this information remains confidential. The parties should also stipulate how the monitor is to return any confidential or proprietary documents upon completion of the monitorship.

114 See s.7.14 of the Code.

See Chapters 5 and 6 on beginning an internal investigation; 7 and 8 on witness interviews; and 13 and 14 on employee rights

It may also be necessary for the monitor to interview personnel, from low-level employees to senior management. The monitorship agreement should ordinarily address issues of employee rights that could arise during the monitorship, including privacy rights and the right to counsel – issues that take on added complexity where the monitor's review is cross-border. Ordinarily, the monitor should inform interviewees of his or her identity and explain why information is being collected. The monitor should also inform interviewees whether they are the target of the monitor's investigation and of their right to have counsel present during the interview. Where an employee chooses to exercise the right to counsel, the monitor must respect that decision.[115]

The monitor may find it advisable to inform interviewees of the degree to which the information being provided will remain confidential and what, if anything, the monitor is required to do with that information. In some circumstances, such as when information would otherwise be hard to extract, it may be appropriate for the monitor to have the authority to collect information confidentiality to protect its sources.[116]

32.5.5 Issuing recommendations and reports

During the course of the monitorship, the corporation and monitor should work together to develop recommendations for improvement of the corporation's compliance programme and to prevent recidivism of corporate misconduct. The recommendations should be mindful of local laws concerning, for example, data privacy and privilege. Depending on the scope and duration of the monitorship, the monitor may summarise his or her findings and recommendations in periodic reports to the government or court, or issue a single report at the end of the monitorship.[117] As negative findings in the report have the potential to significantly harm the corporation, in some circumstances the monitor may provide the corporation with a preliminary draft and invite comments.[118] Ultimately, however, the report is issued by the monitor alone, and must reflect the monitor's honest conclusions and recommendations.

Where the corporation disagrees with one of the monitor's recommendations, the corporation may reject it within a reasonable time, provided the government is informed. The government may consider this rejection when evaluating whether the corporation has fulfilled its obligations under the settlement.[119] Under the

115 Except in limited circumstances, a company is not required to provide counsel or pay for counsel for employees being interviewed.

116 ABA Standards for Monitors § 24-4.2(4)(d).

117 Morford Memorandum, supra note 11, at 6.

118 ABA Standards for Monitors § 24-4.3(1)(d). Giving the corporation the opportunity to review a draft report may improve the quality of the report, as the corporation can correct any errors and, where applicable, provide evidence to rebut the monitor's negative findings.

119 Morford Memorandum, supra note 11, at 6. For example, after Standard Charter settled charges that it disguised transactions that could have violated US sanctions, two monitors were appointed as well as one 'independent consultant'. The monitors' findings that inadequate controls were used led to an additional $300 million fine. Rachel Louise Ensign and Max Colchester, 'Meet

Grindler Memorandum, where a corporation rejects a monitor's recommendation on the basis of cost, it should provide a written proposal of 'an alternative policy, procedure, or system designed to achieve the same objective or purpose'.[120]

In the United Kingdom, the confidentiality of a monitor's reports and correspondence is expressly recognised in the Code, and its disclosure is restricted to the company, the prosecuting authority and the court (except as otherwise permitted by law).[121] Similarly in the United States, the government routinely denies Freedom of Information Act requests filed by news outlets for the production of monitor reports.[122] However, the public's right of access to such reports has been litigated in relation to the deferred prosecution agreement between the DOJ and HSBC.[123]

By way of background, in 2012, HSBC reached a US$1.9 billion settlement with the government and secured a five-year DPA for HSBC's failure to comply with anti-money laundering laws and US sanctions.[124] In an unusual turn of events, the court approved the DPA on the condition that the court could continue to exercise 'supervisory' control over the case.[125] A monitor was appointed as part of the settlement and issued a 1,000-page report in January 2015, a copy of which was filed under seal with the court. Thereafter, an HSBC mortgage customer asked the court to unseal the report so he could determine whether HSBC continued to engage in 'unsafe and unsound business practices'.[126] The lower court held that the report qualified as a 'judicial record' that should be filed publicly, and that 'the public has a First Amendment right to see the Report', though HSBC and the government could suggest redactions and parts to remain under

---

the Private Watchdogs Who Police Financial Institutions', *The Wall Street J.* (30 August 2015), www.wsj.com/articles/meet-the-private-watchdogs-who-police-financial-institutions-1440983917.

120 Grindler Memorandum, supra note 13, § II.

121 See s.7.20 of the DPA Code of Practice.

122 Rachel Louise Ensign and Max Colchester, 'Meet the Private Watchdogs Who Police Financial Institutions', *The Wall Street J.* (30 August 2015), www.wsj.com/articles/meet-the-private-watchdogs-who-police-financial-institutions-1440983917.

123 The HSBC matter represents the most public instance of a party seeking access to a monitor's report, however, it is not the only such example. See *In re Depuy Orthopaedics, Inc. Pinnacle Hip Implant Prod. Liab. Litig.,* No. 11 MD 2244, 2013 WL 2091715 (N.D. Tex. 15 May 2013) (ordering disclosure of monitor's report in a product liability matter).

124 In December 2017, the DOJ found that HSBC had successfully addressed the issues related to its case and sought to dismiss. Evan Weinberger, 'DOJ Seeks Dismissal of HSBC Money Laundering Case', *Law 360* (12 December 2017), https://www.law360.com/articles/993914/doj-seeks-dismissal-of-hsbc-money-laundering-case.

125 See Christie Smythe, 'Judge Lets Sun Shine on Secret HSBC Money Laundering Report', Bloomberg (29 January 2016), www.bloomberg.com/news/articles/2016-01-29/judge-lets-sunshine-on-secret-hsbc-report-on-money-laundering.

126 Nate Raymond, 'HSBC money laundering report's release likely delayed: U.S. judge', Reuters (10 February 2016), www.reuters.com/article/us-hsbc-moneylaundering-idUSKCN0VI28H. See *United States v. HSBC Bank USA NA*, No. 12 CR 763 (JG), 2016 WL 347670, at *1, *6 (E.D.N.Y. 28 January 2016), motion to certify *appeal denied*, No. 12-0763, 2016 WL 2593925 (EDNY 4 May 2016) (inviting the parties to suggest further redactions to the report).

seal.[127] HSBC and the government opposed the unsealing, claiming it 'could provide a "road map" for criminals seeking to launder money'.[128] HSBC's lawyer said the court's order also called into question assurances given to foreign regulators who had provided information to the monitor on condition the report be kept secret.[129] On 12 July 2017, the United States Court of Appeals for the Second Circuit reversed the lower court's decision noting that 'a district court's role vis-à-vis a DPA is limited to arraigning the defendant, granting a speedy trial waiver if the DPA does not represent an improper attempt to circumvent the speedy trial clock, and adjudicating motions or disputes as they arise.'[130] Given the limited supervisory role of courts in the DPA context, the Second Circuit held that a monitor's report is not a judicial record because it is not 'relevant to the performance of the judicial function'.[131] The holding, which relies upon and is consistent with the DC Circuit Court of Appeals' decision in *United States v. Fokker Services BV*, limits both a district court's initial judicial review of a DPA and its subsequent oversight of the DPA's execution.[132]

The District Court for the District of Columbia made a similar ruling in *100Reporters LLC v. United States Department of Justice*, concerning monitor reports issued in the wake of Siemens' 2008 settlement with the United States and Germany. There, reporters sued to obtain the reports under FOIA. In a March 2017 decision, the court acknowledged that significant portions of the report may be exempt from production under FOIA – for example, because they contain 'classic attorney work-product' and 'information [that] cuts to the core of Siemens' business', on which a competitor could rely to Siemens' detriment – but the court was not prepared to find that all information should be so shielded.[133]

Given the remaining uncertainty over the confidentiality of the monitor's report, it has become best practice – as confirmed by ABA Standard 24-4.3(4) – for the government and the corporation to determine whether reports will be made public when negotiating the settlement agreement:

127 *HSBC Bank USA NA*, 2016 WL 34760, at *1, *6. ZTE's monitor reports may be particularly susceptible to this type of argument, given that the plea agreement as amended by Judge Kinkeade refers to the monitor as a 'judicial adjunct' and provides that all monitor reports be filed with the court, albeit under seal and subject to in-camera review. See supra notes 68-72 and accompanying text.

128 Nate Raymond, 'HSBC money laundering report's release likely delayed: U.S. judge', Reuters (10 February 2016), www.reuters.com/article/us-hsbc-moneylaundering-idUSKCN0VI28H.

129 Id.

130 *United States v. HSBC Bank USA, N.A.*, 863 F.3d 125, 129 (2d Cir. 2017).

131 Id. at 137.

132 See *United States v. Fokker Services B.V.*, 818 F.3d 733 (D.D.C. 2016).

133 *100Reporters LLC v. U.S. Dep't of Justice*, No. 14-1264-RC, at 3, 32, 58 (D.D.C. 31 March 2017) (finding that the DOJ had justified withholding portions of the report under certain exemptions to FOIA, but had not justified the withholding of all portions of the report or demonstrated that the report could not be segregated for purposes of partial production).

> *To perform its duties, the monitor needs access to unprivileged, confidential and proprietary business information of the corporation and communications among the corporation, the monitor and the government need to be candid and complete over an extended period.*
>
> *Recognising that corporate information included in monitor reports may be used unfairly by competitors and others to disadvantage the corporation, DPAs and NPAs typically reflect the parties' intentions to maintain the confidentiality of monitor reports.*[134]

Where a proposed settlement agreement instituting a monitorship lacks such explicit proviso for confidentiality, counsel should seek to revise and include it.

Costs and other considerations 32.6

Monitorships can be extremely expensive, with monitors collecting multimillion-dollar fees, to be paid for by the corporation (and ultimately its shareholders).[135] Critics note that the rise in monitorships has created 'a lucrative cottage industry made up of former prosecutors and small consulting firms', some of which even offer expertise in assisting corporations monitor their monitors.[136] Others argue that the cost of the monitorship will be offset against the fines levied on the corporation and that the imposition of a monitor may help sway the government in favour of reduced fines.[137]

---

134 Karen F Green and Timothy D Saunders, 'Minding the Monitor: Disclosure of Corporate Monitor Reports to Third Parties', Bloomberg BNA (2014), available at https://www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/Publications/Documents/green-saunders-minding-the-monitor.pdf.

135 Both the Morford Memorandum and the Grindler Memorandum counsel the need for prosecutors to be mindful of the costs of monitors and their potential impact on the corporation when negotiating settlements. Grindler Memorandum, supra note 13, § II (noting that the government 'should help to instill public confidence in the Department's use of monitors, including the Department's mindfulness of the costs of a monitor and their impact on a corporation's operations'); Morford Memorandum, supra note 11, at 2 (noting that prosecutors must be mindful of 'the cost of a monitor and impact on the operations of a corporation').

136 Rachel Louise Ensign, 'Judge Rules HSBC's Outside Monitor's Secret Report Should be Made Public', *The Wall Street J.* (29 January 2016), www.wsj.com/articles/judge-rules-hsbcs-outside-monitors-secret-report-should-be-made-public-1454086003; see also Rachel Louise Ensign and Max Colchester, 'Meet the Private Watchdogs Who Police Financial Institutions', *The Wall Street J.* (30 August 2015), www.wsj.com/articles/meet-the-private-watchdogs-who-police-financial-institutions-1440983917.

137 Whereas fines are usually due in one lump sum, payments for monitors are commonly billed monthly. See Jason T Wright, 'The Corporate Compliance Monitor's Role in Regulatory Settlement Agreements', SRR (Spring 2014), www.srr.com/article/corporate-compliance-monitors-role-regulatory-settlement-agreements ('More often than not, however, this cost is far less than what the company would otherwise pay in fines, possible debarment, or legal fees in defending an enforcement action through trial.'); Patricia M Sulzbach, 'Independent Corporate Monitors: A Company's Friend or Foe?', ABA White Collar Crime Comm. Newsletter (18 April 2013), available at https://www.americanbar.org/content/dam/aba/publications/criminaljustice/sulzbach.authcheckdam.pdf.

The ultimate cost of the monitorship will largely depend on the scope and duration of the monitorship. Cost will also be influenced by the complexity of the settlement agreement, the state of the corporation's existing compliance programme, and the geographic markets and industries in which the corporation operates. The monitor should take these various factors into consideration when providing the corporation with a projected budget. The monitor and the corporation should also consider and agree on an hourly rate or a fixed rate, any applicable rate adjustments and a potential fee cap. Further, to increase transparency and mitigate the risk of conflicts, the monitor should provide regular updates on the costs being incurred and expected to be incurred.[138]

As one example of the issues that can arise because of costs, in 2014, Apple moved to disqualify its antitrust monitor for what it viewed as excessive billing and unprofessional conduct where the monitor, *inter alia*, had charged a rate of US$1,000 per hour in fees.[139] The motion was denied by the Southern District of New York and affirmed by the Second Circuit, but the Second Circuit noted that the issues raised had 'considerable resonance because the fairness and integrity of the courts can be compromised by inadequate constraint on a monitor's aggressive use of judicial power'.[140]

32.7 Conclusion

Since their first widespread application in the 1990s, the use of monitors has rapidly expanded across industries and offences: banks, energy companies, unions, car manufacturers and fire departments have all been (or currently are) subject to oversight by monitors. Implemented to address a myriad of wrongs ranging from fraud and racketeering to discriminatory hiring practices, monitorships were in many ways viewed as panaceas.

Today, rising costs and increasing concerns about their efficacy have resulted in far greater scrutiny of all proposed monitorships. Where the past two decades represent an expansion in the breadth of cases where monitors were contemplated, the next two are likely to focus on and refine the scope. The ongoing debates over whether monitors' reports should be public, the degree to which monitors are truly independent, and how monitors should be selected will result not only in additional litigation, but will also force an evolution in how monitorships are used as settlement tools. The issues identified throughout this chapter are live controversies, each likely to distil and develop the body of case law governing monitorships, ultimately resulting in a body of jurisprudence that imposes default standards of disclosure, transparency, control and authority on monitors, the government and defendants alike.

138 See also ABA Standards for Monitors § 24-3.4.

139 *United States v. Apple, Inc.*, 992 F. Supp. 2d 263 (S.D.N.Y. 2014).

140 *United States v. Apple, Inc.*, 787 F.3d 131, 133–34 (2d Cir. 2015).

33

Parallel Civil Litigation: The UK Perspective

Nichola Peters and Michelle de Kluyver[1]

Introduction 33.1

The conduct under review in investigations can generate a range of parallel proceedings. These can precede the investigation, follow on from the investigation findings or, frequently, arise in the course of an investigation. It can be a particular challenge to manage parallel proceedings, which engage their own procedural rules and can force the pace of investigations or create other tensions with the investigative process. This chapter deals with the types of issues and parallel proceedings most likely to arise in complex investigations.

Stay of proceedings 33.2

Where a company subject to investigation is also involved in ongoing civil proceedings (before the courts or an arbitral tribunal) that relate to the conduct under investigation, the parties may seek to stay those proceedings pending the outcome of the investigation. This would often be an ideal solution to managing the tensions they introduce but obtaining a stay can be difficult and is not automatic.

Civil litigation 33.2.1

There are many reasons why a court may stay proceedings. For instance, to allow for arbitration, for the dispute to be tried by national courts of another jurisdiction or for other case management purposes (for example, to permit commercial settlement negotiations, or to allow a ruling on a relevant issue to be delivered in

1 Nichola Peters and Michelle de Kluyver are partners at Addleshaw Goddard LLP. Michelle de Kluyver co-authored this chapter for the first edition with Edward McCullagh and would like to thank him for his contribution as co-author and then as author of later editions, as well as Jonathan Hitchin of Allen & Overy LLP for his support on all earlier editions.

a separate case). The court may do so on various legal bases. As well as possessing inherent jurisdiction to manage proceedings,[2] the court is empowered under the Civil Procedure Rules (CPR) to stay proceedings in part or in whole, either indefinitely or until a specified date or event.[3] The court may stay proceedings in specific circumstances pursuant to certain other statutes.[4]

In circumstances where there are related criminal proceedings, the following principles (among others) will apply to the exercise of the court's discretion to stay civil proceedings:[5]

- the court will only consider staying the civil proceedings if there is a real risk of serious prejudice which may lead to injustice;[6]
- the court will exercise its discretion by reference to the competing considerations between the parties – the court has to balance justice between the parties;[7]
- the fact that a defendant, by serving a defence in civil proceedings, would be giving advance notice of their defence in criminal proceedings, carries little weight in the context of an application for a stay of civil proceedings;
- it is not enough that both the civil and criminal proceedings arise from the same facts, or that the defence of the civil proceedings may involve a defendant taking procedural steps (such as exchanging witness statements, and providing disclosure of documents) which might not be imposed on them in the criminal proceedings;[8] and
- even if the court is satisfied that there is a real risk of serious prejudice leading to injustice if the civil proceedings continue, the proceedings should nevertheless not be stayed if safeguards can be imposed in respect of the civil proceedings which provide sufficient protection against the risk of injustice.

In the competition law context, the court may stay proceedings to avoid taking decisions that conflict with decisions contemplated by the European Commission.

The court may also impose a stay on the effects of an action, such as a stay of execution of orders of a lower court pending appeal.

A stay of proceedings puts a stop to their further conduct at the stage they have reached, apart from the taking of any steps allowed by the CPR or the terms of the stay. Proceedings can be continued if the stay is lifted.

2 See, e.g., *China Export & Credit Insurance Corporation v. Emerald Energy Resources Limited* [2018] EWHC 1503 (Comm), [61].

3 CPR, Part 3.1(2)(f).

4 For example, section 9 of the Arbitration Act 1996.

5 See *Akcine Bendrove Bankas Snoras (in bankruptcy) v. Antonov* [2013] EWHC 131 (Comm), [18].

6 *R v. Panel on Takeovers and Mergers, ex parte Fayed* [1992] BCC 524, 531.

7 *Panton and others v. Financial Institutions Services Ltd* [2003] UKPC 95, [11].

8 *FSA v. Anderson* [2010] EWHC 308 (Ch), [19].

Arbitral proceedings 33.2.2

In England, as in many other jurisdictions, procedural matters in arbitration are governed first and foremost by parties' agreement. Aspects of applicable arbitral procedure may be set out expressly in an arbitration agreement, be contained in the parties' chosen institutional arbitration rules (whether such choice is expressed in the arbitration agreement or otherwise) or subsequently be agreed by the parties to a dispute, whether on an *ad hoc* basis or, for instance, in the tribunal's agreed terms of appointment. Where parties do not reach agreement, procedural arrangements are otherwise within the discretion of the arbitral tribunal as a matter of English law, subject to the tribunal's general duties to act fairly and impartially as between the parties and to adopt procedures suitable to the circumstances of the particular case.[9]

An arbitral tribunal may, in exercise of its discretion, elect to stay the arbitral proceedings for a variety of reasons. For instance, at the request of one or both of the parties pending settlement negotiations, upon a party failing to comply with an order to provide security for costs or pending the determination of a preliminary point of law by a court.[10] A tribunal might also stay proceedings to avoid the risk of inconsistent decisions where parallel judicial or regulatory proceedings are ongoing, particularly where such proceedings are ongoing in the same jurisdiction as the arbitral seat. In all cases, a tribunal's decision will depend on the propriety of ordering a stay in all the relevant circumstances, which may, in the regulatory context, depend on the identity of the regulator and the extent to which the outcome of the regulatory investigation is likely to impact the matters at stake in the arbitration itself.

Multi-party litigation 33.3

Under English law, class actions do not feature as part of the parallel litigation landscape to the extent that they do in the United States (in particular, securities litigation). Nonetheless, companies may face civil actions brought by multiple parties in a variety of ways and we describe them for completeness. The two main procedural mechanisms for multi-party litigation envisaged by the CPR are representative actions and group litigation orders.[11] Additionally, a form of collective proceeding exists in the competition law context, although this type of action is still very much in its infancy in the United Kingdom.

Representative actions 33.3.1

Representative actions allow persons, in certain circumstances, to represent others in legal proceedings (the represented persons are not joined to the action as parties). The CPR provide that such actions may be brought where more than one

9 Arbitration Act 1996, sections 33-34.

10 Arbitration Act 1996, section 45.

11 See further *Zuckerman on Civil Procedure: Principles of Practice*, Adrian Zuckerman, 3rd edn. (2013); *Improving Access to Justice through Collective Actions*, Civil Justice Council (2008).

person has the same interest in a claim.[12] Judgments or orders given in representative actions are normally binding on all persons represented in the claim, but may only be enforced by or against non-parties with the court's permission.

Representative actions are not extensively used. The provisions of the CPR relating to such actions are restrictive; in particular, the 'same interest' requirement. A further potential deterrent is that represented persons are not liable for the costs of representative actions, although the court does have jurisdiction to order that costs be paid by a non-party in exceptional circumstances.

33.3.2 Group litigation orders

Where claims give rise to common or related issues of fact or law, the court may make a group litigation order (GLO), which provides for the case management of claims covered by the order.

The GLO will contain directions about the establishment of a group register on which the claims to be managed under the GLO will be entered, and will specify the court that will manage the claims on the register. The GLO procedure is 'opt-in' in nature. Claims must be issued before they can be entered on a group register, and an application for details of a case to be entered on a group register may be made by any party to the case. The management court may set a cut-off date after which no further claims may be added to the group register without the court's permission.

The GLO will also specify the 'GLO issues', which will identify the claims to be managed as a group under the GLO. Judgments or orders given or made in a claim on the group register in relation to the GLO issues are binding on the parties to all other claims on the group register. The court may direct that certain claims on the group register should proceed as test cases.

GLOs have been utilised in a range of different types of dispute, but are not particularly widely used and have been subject to criticism.

33.3.3 Joint claims

Multiple parties can also be joined to the same claim. The CPR give the court a range of powers to add or substitute parties to proceedings.[13] Any number of claimants or defendants may be joined as parties to a claim, and any number of claims may be covered by one claim form (provided those claims can be conveniently disposed of in the same proceedings). However, if a large number of parties are joined, this can lead to practical difficulties.

12 Representative actions may also be brought in more limited circumstances pursuant to CPR, Part 19.7.

13 CPR, Parts 19.1 and 7.3.

Test cases 33.3.4

There is no formal and generally applicable test case procedure before the English courts. However, when faced with large numbers of claims that raise common issues, the courts may use their case management powers to allow certain representative claims (usually selected by the parties) to proceed to determination and stay the remainder. While decisions in test cases have value as precedent, they are not determinative of other cases that raise common issues.

Test case procedures have, however, been introduced in certain specific contexts, for example:

- In appropriate circumstances, claims subject to a GLO may proceed as test cases.
- A pilot scheme was introduced (as part of the implementation of the Financial List), which enables certain claims started in the Financial List to be determined as test cases, without the need for a present cause of action between the parties to the proceedings.[14] The claims must raise issues of general importance in relation to which immediately relevant authoritative English law guidance is needed.

Competition law claims 33.3.5

There are specialised collective proceedings for competition law claims.

Such proceedings may be brought before the Competition Appeal Tribunal (CAT) on a stand-alone basis (in which case, a complainant must prove an infringement of certain competition law rules) or on a follow-on basis (which requires an existing infringement decision from the Competition and Markets Authority (CMA), the CAT on an appeal from a decision of the CMA or the European Commission).

Claims will only be eligible for inclusion in collective proceedings if the CAT considers that they raise the same, similar or related issues of fact and law, and are suitable to be brought in collective proceedings.

Collective proceedings must be commenced by a person who proposes to be the representative in those proceedings, but they can only be continued if the CAT certifies them by making a collective proceedings order. The CAT may only make such an order (1) if it considers that it is just and reasonable for that person to act as a representative in the proceedings and (2) in respect of claims eligible for inclusion in collective proceedings.

The collective proceedings may be:

- 'opt-in' (brought on behalf of those class members who opt in); or
- 'opt-out' (brought on behalf of all class members, except for those who (1) opt out or (2) are not domiciled in the United Kingdom at a specified time, and do not opt in).

Class members can opt in or opt out by notifying the representative.

14 CPR, Practice Direction 51M.

Judgments or orders of the CAT in collective proceedings are binding on all represented persons, except as otherwise specified. The CAT may not award exemplary damages in collective proceedings, and damages-based fee agreements for legal representatives are unenforceable if they relate to such proceedings.

Two proposed sets of opt-out collective proceedings have been brought before the CAT to date. Initially, both were unsuccessful,[15] with the CAT holding in the *Pride* case that the proposed class was too broad, and originally in the *MasterCard* case that the proposed methodology for distributing damages did not reflect the loss suffered by individual members of the class. Nonetheless, arguments in both cases that the representatives were unsuitable failed, and the CAT provided guidance on what it expects from applicants in collective proceedings in future.[16] Recently, the *MasterCard* case was appealed successfully, and the judgment was reversed.[17] The Court of Appeal held that the CAT's position on distributing damages was too narrow. Distribution was a matter for the trial judge to consider once an aggregate award had been made. The CAT was not required to assess individual losses, only whether an aggregate award of damages was suitable for the claims.

As regards costs, the general rule in proceedings before the English courts is that the unsuccessful party will be ordered to pay the costs of the successful party. The CAT, however, has a broader discretion to make any order (at any stage of the proceedings) it thinks fit in relation to the payment of costs, and it may take account of (among other things) the conduct of all parties in relation to the proceedings. Costs will not normally be awarded against represented persons who are not the class representative, except in certain particular circumstances.

Settlement of opt-out (but not opt-in) collective proceedings is regulated by statute and overseen by the CAT (which must approve the terms of any settlement reached). In certain circumstances, collective settlements can also be reached in respect of claims even if a collective proceedings order has not been issued.

33.3.6 Collective redress schemes

The Financial Conduct Authority (FCA) may (under section 404 and sections 404A to 404G of the Financial Services and Markets Act 2000 (FSMA)) make rules requiring certain firms to establish and operate a consumer redress scheme in relation to a widespread or regular failure by such firms to comply with requirements applicable to the carrying on by them of any activity. The relevant requirements include both FCA rules and the general law. The power can be used if it appears to the FCA that, as a result of the failure, consumers have suffered (or may suffer) loss or damage in respect of which a remedy or relief would be available in

15 *Dorothy Gibson v. Pride Mobility Products Ltd* [2017] CAT 9 and *Walter Hugh Merricks CBE v. MasterCard Incorporated and Others* [2017] CAT 16.

16 Collective proceedings in relation to the European Commission's 19 July 2016 decision (Case AT.39824 – Trucks), concerning a cartel in the truck manufacturing industry have commenced. *UK Trucks Claim Limited v. Fiat Chrysler Automobiles N.V. and Others* is listed for December 2019 following the pre-hearing review in May 2019.

17 *Walter Hugh Merricks CBE v. MasterCard Incorporated and Others* [2019] EWCA Civ 674.

legal proceedings, and the FCA considers that it is desirable to make rules to secure redress for consumers in respect of the failure. In addition, pursuant to section 404F(7) of FSMA, the FCA may vary the permission or authorisation of a firm to require it to establish and operate a scheme that corresponds to, or is similar to, a consumer redress scheme. The FCA also has administrative powers to require restitution under section 384 of FSMA, which it has previously used to establish a compensatory scheme for investors who suffered loss in connection with an overstatement of expected profits by Tesco plc in 2014.[18]

The FCA has used its power under section 404 of FSMA to introduce rules on consumer redress schemes in the CONRED section of its handbook. In addition to providing general rules on consumer redress schemes, CONRED also sets out in Chapter 2 the rules and key documents of the Arch cru Consumer Redress Scheme.[19] In practice, a great many more redress programmes are conducted by firms under supervision of the FCA or a skilled person appointed by the FCA without use of section 404 of FSMA or CONRED.

Statutory voluntary redress schemes have also been introduced in the competition law context, under which compensation may be offered by businesses as a result of infringement decisions made in respect of them. Such schemes are subject to the approval of the CMA.

Derivative claims and unfair prejudice petitions 33.4

Derivative claims 33.4.1

Members of a company can bring a derivative claim (pursuant to Part 11, Chapter 1 of the Companies Act 2006 (CA 2006)) in respect of a cause of action vested in the company, and seeking relief on its behalf. Such claims may only be brought in respect of a cause of action arising from an actual or proposed act or omission involving negligence, default, breach of duty or breach of trust by a director of the company, and the cause of action may be against the director or another person (or both).

A member who brings such a derivative claim must apply for permission to continue it, and the CPR envisage a two-stage procedure for dealing with applications for permission to continue derivative claims (the company, and any other appropriate parties, are made respondents to the permission application at the second stage).

The court must take into account a number of particular factors when considering whether to grant permission, including the importance that a person acting in accordance with section 172 of the CA 2006 (duty to promote the success of the company) would attach to continuing the claim, and any evidence as to the views of members of the company who have no personal interest (direct or

18 FCA Final Notice to Tesco plc and Tesco Stores Limited dated 28 March 2017.

19 FCA, Consumer Redress Schemes sourcebook, Chapter 2.

indirect) in the matter. However, permission must be refused in certain circumstances (for example, if the act or omission giving rise to the cause of action has been authorised or ratified).

Part 11 of the CA 2006 also includes a mechanism for members to apply (in appropriate circumstances) for permission (1) to continue as derivative claims certain claims brought by the company or (2) to continue derivative claims brought by other members of the company.

33.4.2 Unfair prejudice petitions

A member of a company may also apply to the court for an order under Part 30 of CA 2006 on the grounds that the company's affairs are being or have been conducted in a manner that is unfairly prejudicial to the interests of members generally, or of some part of its members (including at least the applicant), or that an actual or proposed act or omission of the company (including an act or omission on its behalf) is or would be so prejudicial.

The courts take a wide view of prejudice suffered by a shareholder, which need not be financial. The courts also have a very wide discretion in respect of what constitutes unfairness, although they do 'not sit under a palm tree'.[20] Typically, a member will not be entitled to complain of unfairness unless there has been some breach of the terms on which the member agreed that the company's affairs should be conducted, although there will be cases in which equitable considerations will make it unfair for those conducting the company's affairs to rely on their strict legal powers.

The court has a wide discretion to make such order as it thinks fit for giving relief in respect of the matters complained of in an unfair prejudice petition. The most common order in practice is for the shares of the petitioner to be bought by the respondent at a price to be fixed by the court.

As unfair prejudice petitions generally raise numerous factual issues entailing examination of events over a considerable period of time, a high degree of case management is required. In circumstances where a buy-out order is sought, the court will normally determine issues necessary to decide whether a buy-out order should be made at a liability hearing, and only proceed to a quantum hearing if it has been determined that a buy-out order should be made.

33.4.3 Practical considerations

Typically derivative claims and unfair prejudice petitions are brought by minority shareholders.[21] There are a number of practical advantages for such shareholders to bringing an unfair prejudice petition instead of a derivative claim. These include the broad grounds for relief, the flexible nature of the relief and the fact that there are fewer procedural hurdles to overcome. There may be significant

20 *In re J. E. Cade & Son Ltd.* [1992] B.C.L.C. 213, 227.

21 See further *Minority Shareholders: Law, Practice and Procedure*, Victor Joffe QC, David Drake, Giles Richardson, Daniel Lightman and Timothy Collingwood, 6th ed. (2018).

disadvantages in bringing a derivative claim: the initial procedural phases can be costly, and relief must be sought on behalf of the company. However, in certain circumstances a derivative claim may still be the most appropriate route for shareholders (for example, in the context of public companies, where a finding of unfair prejudice may be less likely).

In a derivative action, the court may order the company, for whose benefit the action was brought, to indemnify the claimant against the costs it reasonably incurs. By contrast, in unfair prejudice proceedings, the company is not usually ordered to pay any costs.

The company may be required to give disclosure in the context of derivative claims and unfair prejudice petitions. A shareholder will be entitled to disclosure of documents obtained by the company in the course of the company's administration (where relevant), including advice by solicitors to the company about its affairs, but not where that advice relates to hostile proceedings between the company and its shareholders.

Securities litigation 33.5

As noted above, securities litigation[22] in England and Wales is relatively under-developed in comparison with the position in the United States. However, there are a number of ways in which investors in securities can seek relief before the English courts, and in recent years there has been an increase in the volume of such litigation, due in part to the growing role of third-party litigation funders and specialist claimant law firms.

FSMA sets out the framework for financial services regulation in England and Wales. Section 90 of FSMA imposes liability on issuers and other specified persons (such as the directors of a corporate issuer) where untrue or misleading statements are made in listing particulars or a prospectus relating to certain securities, or where required information is omitted from such documents (or supplementary documents are not published when required), and loss is suffered by investors in respect of those securities as a result. A number of exemptions from such liability are set out in Schedule 10 of FSMA (for instance, where the defendant reasonably believed that the particular statement was true and not misleading, and continued in this belief until the relevant securities were acquired). Section 90A of FSMA applies to broader categories of published information relating to securities, making an issuer liable to pay compensation to investors who suffer loss in respect of those securities as a result of a misleading statement or dishonest omission in that information, or a dishonest delay in publishing information (although liability under section 90A is in some respects more restricted than under section 90 – for instance, the standard of fault under section 90A is higher, and it is necessary to show reliance).[23] In addition, section 138D of FSMA provides a right of action

22 See further *The Securities Litigation Review*, ed. William Savitt, 5th edn. (2019).

23 The high-profile *RBS Rights Issue* litigation involved claims under section 90 of FSMA; and, in more recent litigation arising out of an overstatement of expected profits by Tesco plc in 2014, claims have been made under section 90A of FSMA. (See also Section 33.3.6.)

before the courts for private persons who suffer loss as a result of a contravention by an authorised person of certain chapters of the FCA Handbook. Rules made by the Prudential Regulation Authority may also provide that private parties have a similar right of action. Further, a number of other provisions in FSMA (for example, sections 26, 27 and 30) can render agreements or transactions unenforceable, and give rights to recover money (or other property) and to obtain compensation, where the circumstances in which those agreements or transactions were entered into contravene certain rules in FSMA (for instance, if necessary authorisation from the FCA has not been obtained).

Aggrieved investors may also have other options, in addition to reliance on FSMA. Misrepresentation claims pursuant to section 2(1) of the Misrepresentation Act 1967 may be available to investors in circumstances where the investor enters into a contract in reliance on a misrepresentation made to them by another party to the contract, which causes loss, and where the representor did not have a reasonable belief at the time the contract was made that the facts represented were true. Investors may also be able to bring a negligent misstatement claim (in circumstances where a duty of care is owed to the investor, that duty has been breached and that breach causes the investor to suffer recoverable loss), or a claim based on the tort of deceit (which requires, among other things, proof that the defendant knowingly or recklessly made a false representation).[24]

33.6 Other private litigation

33.6.1 'Tainted' contracts

Conduct which is illegal or contrary to public policy (and which may well be the subject of an investigation) may 'taint' contracts entered into by a company.

The common law doctrine of illegality may prevent a party to a contract tainted by illegal conduct from enforcing their contractual rights and remedies in certain circumstances. Historically, the law in this area has been complicated and unclear, but it was recently reconsidered by nine Supreme Court justices in the case of *Patel v. Mirza*.[25] The majority held that the essential rationale underpinning the illegality doctrine is that it would be contrary to the public interest to enforce a claim if to do so would harm the integrity of the legal system. They identified the following three factors which must be taken into account when considering whether to allow a claim which is in some way tainted by illegality:

- the underlying purpose of the prohibition that has been transgressed, and whether that purpose would be enhanced by denial of the claim;
- any other relevant public policy on which the denial of the claim may have an impact; and

24 In addition to private enforcement, public enforcement proceedings may also be brought against companies (typically by the FCA) for breach of securities rules.

25 [2016] UKSC 42.

- whether denial of the claim would be a proportionate response to the illegality. When considering proportionality, the majority held that (among other things) the seriousness of the conduct, its centrality to the contract, whether it was intentional and whether there was a marked disparity in the parties' respective culpability may potentially be relevant.

This approach was, however, criticised by the minority on the basis that it was too vague and too wide, converting a legal principle into the exercise of judicial discretion. It remains to be seen how the doctrine will develop in light of this important case. For instance, in some more recent decisions, the courts have continued to have reference to case law that pre-dates *Patel*.[26]

Civil law bribery

If bribery has occurred, then a number of particular civil law consequences may also follow.

Civil law bribery[27] arises in the context of agency relationships, where an agent receives a benefit which puts them in a position where their duty (to their principal) and their (personal) interest conflict. The benefit does not necessarily have to be monetary, or provided directly to the agent, and there is no need to prove motive, inducement or loss up to the amount of the bribe. The bribe need not be linked to a particular transaction (provided the agent is tainted by bribery at the time of the relevant transaction between the briber and the principal), and it may taint subsequent transactions. An arrangement will not constitute a bribe in the absence of secrecy, although it may still amount to a breach of fiduciary duty on the part of the agent if the principal's fully informed consent is not obtained.

A variety of alternative remedies are available to a principal faced with civil law bribery.

As against the bribed agent

- If the bribe has been paid to the agent, the principal is entitled to recover the amount of the bribe (at common law, in an action for money had and received), regardless of whether the principal elects to rescind any 'tainted' contracts. The proceeds of bribe-taking (which comprise money or other property) will also be held on trust for the principal, and the principal will have a proprietary remedy in respect of them.
- In the alternative, the principal can claim damages in tort in respect of loss sustained by the principal in consequence of entering into any 'tainted' contracts.
- There may also be other consequences for the agent (including in connection with their contractual relationship with the principal).

26 See, for example, *Henderson v. Dorset Healthcare University NHS Foundation Trust* [2018] EWCA Civ 1841 (appeal outstanding).

27 See further *Bowstead and Reynolds on Agency*, ed. Peter Watts QC, 21st edn. (2017).

As against the briber

- The briber is jointly and severally liable with the bribed agent in respect of the amount of the bribe, which the principal can claim in a common law action for money had and received.
- In the alternative, the briber is also jointly and severally liable with the bribed agent to the principal for damages in tort (see above).
- The principal may have an action for dishonest assistance in a breach of fiduciary duty against the briber.
- Other remedies may be available against the briber (or others) depending on the particular circumstances of the case.

Note that double recovery by the principal from the bribed agent and the briber will not be permitted.

If it can be established that bribery has occurred, then the principal is usually entitled to rescind contracts 'tainted' by the bribery. If the principal elects to rescind a 'tainted' contract, they remain entitled to recover the bribe, and they are not bound to give credit in the rescission for the amount of any bribe recovered. If the agent is bribed during the course of performance of a contract (i.e., after it has been entered into), then the principal may bring it to an end as from the moment of discovery (i.e., for the future); and the same will apply if bribery was effected at the time a 'tainted' contract was entered into, but (for some reason) rescission *ab initio* is impossible. Where an arrangement would have constituted bribery, but the principal is aware of it (so there is no secrecy) although the principal's fully informed consent has not been obtained, then the court may award rescission of 'tainted' contracts as a discretionary remedy, if it is just and proportionate to do so.

Where bribes have been paid to the detriment of a third-party competitor, it has been suggested that both the briber and the company that awards the contract to the briber could be liable to the unsuccessful competitor. Further, if the contract involves a public authority, the unsuccessful competitor may have an action for misfeasance in public office.

A contract to commit bribery (as opposed to a contract procured by bribery) is 'tainted' by illegality, in the sense that it is illegal in performance, and is unenforceable.

33.6.2 Specific provisions in commercial contracts

Parties often include specific provisions in their commercial contracts (including finance documents) aimed at preventing, or providing contractual protection in relation to, illegal behaviour (in particular, corruption) involving a party to the agreement. Accordingly, the fact of an investigation (or related proceedings), or conduct which is the subject of an investigation, may have adverse contractual consequences for a company. These will naturally depend on the nature of both the investigation itself and the specific conduct under investigation, as well as the provisions of the contractual documentation. However, by way of illustration, many commercial contracts contain:

- obligations:
  - to comply with certain applicable laws and regulations;
  - to have in place and comply with specified policies (such as data protection, cybersecurity, anti-slavery and human trafficking or anti-bribery and corruption policies);
  - to maintain accurate records of payments made in relation to the contract;
  - relating to data protection (for example, to prevent damage, or unauthorised or unlawful access, to relevant data);
  - in relation to subcontractors (for instance, to ensure that subcontractors comply with requirements equivalent to those imposed on the company), and that may impose responsibility on the company for any non-compliance by a subcontractor with such requirements;
  - to report generally on compliance to contractual counterparties on an ongoing basis, which could include requiring the provision of a confirmation signed by an officer of the company. Audit rights may also be granted to contractual counterparties; and
  - to report the occurrence of certain events to contractual counterparties. These could include dealing with a public official in connection with the performance of the contract, receiving a request for a payment (or other advantage) in connection with the performance of the contract, or the commencement (or threat) of an investigation into the activities of the company;
- representations (given by the company, and which may be repeated) that it has not been investigated for or convicted of certain offences (and that no proceedings or investigations are pending or threatened), or which relate to the accuracy and completeness of information provided to contractual counterparties;
- termination rights for contractual counterparties if the company breaches (or, potentially, if the contractual counterparty reasonably suspects a breach of) certain obligations, or if the company makes a false representation or is convicted of certain offences; and
- indemnities (for the benefit of contractual counterparties) in respect of loss suffered as a result of a certain breaches of the contract by the company.[28]

A company may face parallel litigation brought by its contractual counterparties in reliance on such provisions. A company may also be able to invoke such provisions against its contractual counterparties, although where a company is under investigation it may not wish to take the position in civil proceedings that its counterparty has engaged in illegal activity if the company is also exposed for its counterparty's conduct.

28 An indemnity against a criminal liability may, however, be unenforceable for public policy reasons.

33.6.3 Mergers, acquisitions and investments

Mergers, acquisitions and investments[29] can present particular risks for companies. Illegal behaviour in the target (or its subsidiaries, or other related companies and persons) may have various negative consequences for an acquiring entity, which can include (1) financial consequences (for example, the target may have been overvalued), (2) legal consequences (both civil and criminal) for the target, the acquiring entity and relevant individuals (including officers of both entities), along with associated legal costs and (3) other practical consequences (for example, reputational damage, which may have a consequent effect on business).[30]

As a result, acquiring entities will often take precautions to minimise these risks. Typically, these include:

- conducting proportionate pre- and post-acquisition due diligence of the target and its business;
- implementing compliance programmes; and
- including appropriate protections in the relevant contractual documentation.

In relation to the latter, warranties, representations and indemnities[31] designed to provide such protection are frequently included in share purchase agreements. The scope of protection will depend on the particular provisions negotiated, but they can be widely drafted, such that they encompass the conduct of, for example:

- the target and its subsidiaries;
- directors, officers, employees, significant shareholders, affiliates, agents, and distributors of the target and its subsidiaries;
- those associated with or acting on behalf of the target and its subsidiaries; and
- those who perform services for or on behalf of the target and its subsidiaries,

and may cover areas such as:

- compliance with laws generally;
- compliance with anti-money laundering laws and standards;
- compliance with anti-bribery and corruption laws and standards;
- debarment from public contracts;
- sanctions (including whether such persons are, have been, or are likely to become, subject to sanctions); and
- whether such persons are (or have been) subject to an investigation or any proceedings, or whether an investigation or any proceedings in respect of such persons are pending, threatened, contemplated, or even likely.

29 See further *Anti-Bribery Due Diligence for Transactions: Guidance for Anti-Bribery Due Diligence in Mergers, Acquisitions and Investments*, Transparency International UK (2012).

30 Companies should also be aware of the risk that illegal behaviour (for example, bribery) may occur during the merger, acquisition or investment transaction.

31 However, see footnote 28, above, in relation to indemnities against criminal liability.

Accordingly, the existence of an investigation (or related proceedings), or conduct which is the subject of an investigation, may give the acquiring entity contractual rights which it can seek to enforce (including through litigation or arbitration). Again, however, care may need to be taken in doing so, for the reasons given in Section 33.6.2.

Defamation proceedings 33.6.4

A company may face defamation actions[32] brought by individuals arising from internal investigations carried out by the company. In particular, issues may arise if it becomes necessary to negotiate an exit from the organisation for individuals involved or implicated in conduct which was the subject of an investigation.

The law of defamation is concerned with the protection of reputation. It covers the torts of libel (which concerns more permanent forms of publication) and slander (which concerns more transient forms of publication, such as speech, and generally is actionable only if special damage can be shown).

Broadly speaking, a defamatory statement is one whose publication has caused, or is likely to cause, serious harm to the claimant's reputation, although a number of different tests have been utilised by the courts when determining whether a statement is defamatory. The statement must have been published (communicated) to a third party, and each publication will amount to a separate cause of action. Liability for publication extends to those who participate in or authorise publication, and those who re-publish or repeat the relevant statement are liable as if the statement originated from them. However, defences are available in certain circumstances to persons who publish statements and who are not the author, editor or publisher (in the sense of being a commercial publisher) of the relevant statement; as well as to website operators, if they can show that the relevant statement was posted on the website by another.

A number of defences may be available to a company facing a defamation action. For example, it may be able to rely on absolute privilege, which will exist where a statement or conduct can fairly be said to be part of the process of investigating a crime (or a possible crime) with a view to a prosecution (or a possible prosecution) in respect of the matter being investigated. This applies to statements made by persons assisting an inquiry to investigators, and by investigators to those persons or to each other. Absolute privilege will also extend beyond the criminal context, to certain enquiries made in connection with proceedings before a tribunal, the proceedings of which are protected by absolute privilege (i.e., tribunals acting in a manner similar to that in which a court of justice acts). Accordingly, the provision of information by a company to the authorities in connection with an investigation is unlikely to expose that company to the risk of a defamation action. The defence of qualified privilege will also be available in circumstances where the maker of a statement has a legitimate interest or duty in making it to

32 See further *Gatley on Libel and Slander*, eds. Alastair Mullis and Richard Parkes QC, 12th edn. (2013).

the recipient, and the recipient has a corresponding interest or duty in receiving it, provided the maker is not motivated by malice. This may apply to certain communications between an employer and their employees, or between employees, that relate to the employer's business.

A company may also, in theory, be in a position to bring a defamation action against a whistleblower, given that the act of blowing the whistle will typically involve the publication of a statement that causes harm to reputation. Nonetheless, under the Defamation Act 2013, to satisfy the serious harm threshold, a company must show that the publication caused or is likely to cause serious financial loss. Whistleblowers may, however, be able to make out one or more possible defences to such a claim. In particular:

- if the whistleblower can show that the statement was substantially true, this will generally constitute a defence to a defamation action; and
- whistleblowers may also benefit from the defence of absolute privilege (as set out above) or qualified privilege, provided that they are not motivated by malice. It is notable, however, that the Public Interest Disclosure Act 1998 does not provide protection from a defamation action for a whistleblower, although if such an action were brought by an employer this is likely to amount to a 'detriment' for the purposes of section 47B of Part V of the Employment Rights Act 1996.[33]

In addition, a company may be in a position to bring a defamation action in relation to press comment although litigation could have the effect of drawing attention to the allegation, which is seldom beneficial.

The primary remedy in defamation actions is the award of damages, and claimants may also seek an injunction against repetition of the publication complained of. In addition, the court may order the defendant to publish a summary of the court's judgment, and may also order others to stop distributing, selling or exhibiting material containing the relevant statement, or to remove the relevant statement from a website on which it is posted. Particular remedies are available where the claimant is granted summary relief.

Although in the past trial by jury was typical in defamation actions, the right to jury trial has recently been abolished in this context, and trial will now be by judge save in exceptional circumstances.

33.6.5 Arbitration

Allegations of unlawful behaviour can have a significant impact in the context of international arbitration,[34] both before a tribunal itself and before national courts at the stage of recognition or enforcement of an award.

33 See further *Whistleblowing: Law and Practice*, John Bowers QC, Martin Fodder, Jeremy Lewis and Jack Mitchell, 3rd edn. (2017).

34 See further *International Commercial Arbitration*, Gary Born, 2nd edn. (2014).

In the context of commercial arbitration, as in the context of civil ligation, allegations of unlawful conduct can impact parties' disputed rights and obligations under the applicable law in myriad ways. Should a regulatory body, for instance, determine a party's conduct to be unlawful, this might be taken into account by a tribunal in its consideration of claims of invalidity of a contract on grounds of illegality. In the context of recognition and enforcement of foreign arbitral awards, unlawful conduct may impact a court's assessment of a party's claims to resist recognition or enforcement on the grounds set out in Article V of the New York Convention, for instance, on public policy grounds.[35]

A party's unlawful conduct can also have a significant impact in the context of determination of investor–state disputes arising under international treaties. In particular, numerous international tribunals have been faced with assessing allegations of investor misconduct, often involving corruption or bribery, in a variety of contexts. The findings of a domestic regulatory body, while compelling evidence of unlawful conduct under the law of the regulator's jurisdiction, are only one factor to be taken into account by an international tribunal. The consequences of unlawful conduct under a domestic law being proven to the satisfaction of an international tribunal will vary, and often depend to a large extent on the provisions of the treaty or other instrument under which the claim has been brought. In general terms, however, there is an emerging consensus in international practice that investment claims tainted by corruption or other unlawful conduct will be dismissed on grounds of inadmissibility (or, according to some tribunals, for lack of jurisdiction). Where investment treaty awards are governed by the New York Convention, the same considerations apply with respect to enforcement and recognition as for commercial awards.

Employment law and whistleblowing 33.6.6

Investigations can have employment law consequences for a company. Employees may seek to bring claims against their employers arising out of the subject matter of an investigation, or how the investigation is handled; conversely, an employer may wish to take action against an employee implicated in the conduct under investigation.

See Chapter 13 on employee rights

In addition, to the extent that allegations have been made by whistleblowers, companies under investigation or conducting investigations should be careful to respect whistleblower rights to avoid claims for breach of the protections afforded to whistleblowers. For a disclosure by an employee to be protected, it must be made where the employee has a reasonable belief that the information tends to show breach of a legal obligation, in the public interest and to a prescribed person.

See Chapter 19 on whistleblowers

35 Convention on the Recognition and Enforcement of Foreign Arbitral Awards 1958, Article V(2)(b); Arbitration Act 1996, section 103(3)

33.6.7 Data breaches

The General Data Protection Regulation[36] (GDPR) has applied in the United Kingdom since 25 May 2018, and makes provision for the protection of natural persons with regard to the processing of personal data, and the free movement of such data. In addition to the penalties that may be imposed by supervisory authorities pursuant to the GDPR,[37] which can include an administrative fine of up to €20 million or up to 4 per cent of an undertaking's total worldwide annual turnover of the preceding financial year (whichever is higher) in respect of certain infringements, companies that are data controllers or processors may also face actions brought by data subjects in respect of infringements of their rights under the GDPR (data subjects may mandate representative organisations to bring actions on their behalf), as well as actions for compensation brought by any persons who have suffered damage as a result of an infringement of the GDPR.[38]

Relatedly, the GDPR also requires notification of certain personal data breaches to the competent supervisory authority without undue delay, and in certain circumstances communication to the data subject is also necessary.[39] Even in cases not involving personal data, companies may face significant regulatory consequences following cyberattacks – in 2018, the FCA imposed a fine of £16.4 million on Tesco Bank following a cyberattack in November 2016, which did not involve the loss or theft of personal data.[40]

Companies may also be responsible for data breaches by rogue employees. It was recently held, in the context of a group action brought by more than 5,500 employees of a supermarket company whose personal information was disclosed by the actions of a disgruntled IT auditor employed by the company, that the company was vicariously liable for the actions of that IT auditor, even though the company itself had not breached applicable data protection rules.[41]

36 Regulation (EU) 2016/679.

37 In the United Kingdom, the relevant authority is the Information Commissioner's Office.

38 See GDPR, Articles 79, 80, 82 and 83. The courts recently did not permit a broad representative action against Google to proceed, in which the representative claimant sought compensation which was estimated as being in the range from £1 billion to 3 billion (*Lloyd v. Google LLC* [2018] EWHC 2599 (QB)). It was argued that Google had acted in breach of a duty imposed by the Data Protection Act 1998 (allegedly by secretly tracking the internet activity of Apple iPhone users, and using and selling the accumulated data), but the court found (among other things) that, on the facts alleged, relevant damage had not been suffered, and that class members did not have the same interest. The appeal by the class members is outstanding.

39 GDPR, Articles 33 and 34.

40 FCA Final Notice to Tesco Personal Finance plc dated 1 October 2018.

41 *Wm Morrison Supermarkets Plc v. Various Claimants* [2018] EWCA Civ 2339. Application for permission to directly appeal to the Supreme Court was granted and the appeal is outstanding.

Evidentiary issues 33.7

Reliance by the court on findings made by the authorities 33.7.1

Parties may seek to rely on findings made by the authorities in an investigation (such as a final notice from the FCA) in subsequent civil litigation. Objections may be raised to such reliance on the grounds of admissibility – as a matter of evidence, bare findings made in earlier proceedings are ordinarily inadmissible and excluded under what is known as the rule in *Hollington v. Hewthorn*,[42] although this controversial rule is subject to exceptions, and it has been held that a court can take into account the substance of underlying evidence as set out in prior decisions (giving it such weight as is appropriate).[43] In addition, a court may allow documents containing other relevant evidence, in addition to inadmissible findings, to be put before the court, with the judge taking into account that which is admissible and ignoring that which is inadmissible.[44]

Some investigations may result in criminal prosecutions and, potentially, convictions. In any subsequent civil proceedings, the fact of a UK conviction will be admissible in evidence for the purpose of proving, where relevant, that the convicted person committed the offence, and the information, complaint, indictment or charge sheet on which the person in question was convicted are admissible for the purpose of identifying the facts on which the conviction is based.[45] Where criminal proceedings follow civil proceedings, ordinarily findings of a civil court on the matters in issue in the criminal case will not be admissible in those subsequent criminal proceedings, although in some circumstances civil judgments may be admissible pursuant to the rules concerning evidence of bad character.

In addition, if a company enters into a deferred prosecution agreement (DPA) with a prosecutor, this must contain a statement of facts relating to the alleged offence and the company will be required to admit the contents and meaning of key documents referred to in the statement of facts.[46] Parties which bring civil litigation against the company may seek to rely on the contents of a DPA statement of facts as having the status of admissions by the company and may also seek disclosure of any underlying documents.

Certain specific rules apply in the competition law context. Pursuant to EU law, national courts may not make determinations which conflict with European Commission decisions (or rulings of both the General Court and the European Court of Justice) on certain EU competition law issues. Where no risk of direct conflict arises, but a decision of the European Commission addresses similar subject matter to that before the national court, the European Commission decision may simply be admissible as evidence before the national court (although, given the expertise of the European Commission, it might well be regarded by that

42 *Hollington v. F Hewthorn & Co Ltd* [1943] KB 587.

43 See e.g. *JSC BTA Bank v. Ablyazov & Anor* [2018] EWHC 1368 (Comm), [19].

44 *Rogers v. Hoyle* [2014] EWCA Civ 257, [53]–[55].

45 Civil Evidence Act 1968, section 11.

46 Crime and Courts Act 2013, Schedule 17, paragraph 5(1); Deferred Prosecution Agreements Code of Practice, para. 6.1.

court as highly persuasive). The Damages Directive, which was implemented in the United Kingdom in March 2017, provides that final decisions of national competition authorities (or review courts) in other Member States may be presented before national courts as at least *prima facie* evidence that an infringement of competition law has occurred. In addition, the Competition Act 1998 (as amended) provides that findings of fact made by the CMA during the course of an investigation (which have not been appealed, or which have been confirmed on appeal) which are relevant to an issue arising in certain competition law proceedings before the High Court (or the CAT) are binding on the parties to those proceedings, unless the court (or the CAT) orders otherwise. Further, where a claim is brought before the High Court (or the CAT) in respect of an infringement decision (from the CMA, the CAT on an appeal from a decision of the CMA or the European Commission), the court (or the CAT) is bound by that infringement decision once it has become final.

33.7.2 Reliance by an authority on court findings

Matters which come to light during the course of civil litigation can have repercussions beyond the immediate context of those proceedings. They may draw the attention of the authorities, and there have been cases where authorities have relied on the findings of civil courts as grounds for taking action. For example, the FCA has previously prohibited individuals from carrying on regulated activities on the basis of findings in High Court judgments (in one instance, without conducting a separate investigation).[47] Accordingly, these risks may be relevant considerations for a company when considering and implementing its litigation strategy in civil proceedings. In addition, conflict and privilege issues may arise if the interests of the company and its employees are not aligned.

33.7.3 Collateral use of disclosed documents

English law can impose onerous disclosure obligations on parties to civil proceedings – typically, parties are required to disclose documents on which they rely, and documents which adversely affect their case, adversely affect another party's case or which support another party's case (although the court may make an alternative order in relation to disclosure, and a pilot scheme involving generally less expansive disclosure obligations to apply in the Business and Property Courts in England and Wales for two years was rolled out in January 2019[48]). In certain circumstances, parties may protect documents from inspection, for instance, on the grounds of privilege or the public interest. However, the confidentiality of a relevant document is not, of itself, a justification for refusing to disclose it, although it may be relevant to the exercise of the court's discretion to order

47 FCA Final Notice to Mr Anthony Verrier, dated 27 January 2014; FCA Final Notice to Mr Stephen Robert Allen, dated 14 April 2015; *Stephen Robert Allen v. The Financial Conduct Authority* [2014] UKUT 0348 (TCC).

48 See Disclosure Pilot for the Business and Property Courts Press Announcement, dated 31 December 2018, accessible on www.judiciary.co.uk and CPR Practice Direction 51U.

disclosure. Although certain recent decisions of the English courts regarding the law of privilege had pointed towards a more restrictive interpretation of the scope of the protection which it offers,[49] the important judgment of the Court of Appeal in the *ENRC* case (concerning, in particular, the scope of litigation privilege in the context of a corruption investigation) suggests that this trend is beginning to change.[50]

As a result, a company involved in civil proceedings may be required to disclose sensitive documents to an opponent, including documents relevant to an investigation or even unprivileged investigation material.

The impact of the invasion of a litigant's right to privacy and confidentiality which the obligation to give disclosure constitutes is mitigated to some extent by CPR Part 31.22, which provides that where a document has been disclosed to a party, that party may only use the document for the purpose of the proceedings in which it is disclosed, except where:

- the document has been read to or by the court, or referred to, at a hearing held in public (although the court may make an order restricting or prohibiting the use of such a document);
- the court gives permission; or
- the party who disclosed the document and the person to whom the document belongs agree.[51]

The court will only grant permission if there are special circumstances which constitute a cogent reason for permitting collateral use. Permission decisions are highly fact-sensitive – the proposed collateral use for the document will be relevant, and, depending on the proposed use, the court may carefully consider the particular documents in respect of which permission is sought.

If the court gives permission for collateral use, a party will be able to deploy the material outside the context of the civil proceedings. The court may make an order that they could be used in separate proceedings (including abroad). Once documents are moved outside the jurisdiction of the United Kingdom, there is a risk that they may be seized or that the party in possession of them may be compelled under local laws to produce them to third parties. Similar concerns about losing control over documents may arise where documents have been provided to regulatory or enforcement authorities during the course of an investigation. Even

49 See, for example, *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch), and the first-instance decision in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corp Ltd* [2017] EWHC 1017.

50 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corp Ltd* [2018] EWCA Civ 2006; see also *Bilta (UK) Ltd v. Royal Bank of Scotland* [2017] EWHC 3535 (Ch) (concerning litigation privilege) and *Property Alliance Group Limited v. The Royal Bank of Scotland Plc* [2015] EWHC 3187 (Ch) (in the legal advice privilege context).

51 See *Tchenguiz v. Grant Thornton* [2017] EWHC 310 (Comm) for the broad interpretation of collateral 'use' in relation to CPR Part 31.22, which includes, for example, reviewing documents for relevance; and see also *The ECU Group Plc v. HSBC Bank Plc & Ors* [2018] EWHC 3045, in which the judge emphasised the importance of the rule in CPR Part 31.22.

where documents are shared with an authority on a conditional basis, the authority may share the documents with third parties if it believes it has a statutory duty to do so. There is also the risk that the authority will be required to disclose those documents if it becomes involved in civil proceedings.

33.8 Practical considerations

33.8.1 Coordination with internal investigations team

It is important that those within the company responsible for managing parallel civil litigation are in constant communication with the internal team responsible for dealing with investigations, to ensure that:

- a clear, holistic strategy is developed for managing the investigations and parallel civil proceedings, and anticipating areas of potential risk (e.g., possible civil claims which may arise but have not yet been commenced);
- both teams understand, and evaluate the risks of, new developments in both the criminal and civil spheres; and
- any proposed action by the company or associated persons, in the civil or criminal spheres, is carefully analysed to determine the potential repercussions for all other proceedings and investigations.

Issues can arise, for instance, where:

- an authority seeks disclosure of privileged documents from the company in circumstances where the company may wish to assert privilege over those documents in subsequent civil proceedings;
- witnesses, whose testimony may be important for the company's case in civil proceedings, are under investigation, or have been classified as suspects, by the authorities, and have concerns about self-incrimination. Depending on the circumstances, employment proceedings may also be ongoing in respect of such individuals;
- pleading possible defences (such as illegality) in civil proceedings, which may strengthen the company's case in those proceedings but would undermine the position it has taken in relation to an investigation;
- (as part of DPA negotiations) there is a risk that matters which an authority seeks to include in an agreed statement of facts could be relied upon against the company in parallel civil proceedings. Conversely, any settlement agreement relating to civil proceedings may be disclosable to an authority as part of their investigation; or
- suspicious activity is identified in the course of civil proceedings (e.g., during disclosure) which the company is then obliged to disclose to the investigating authority.

See Chapter 7 on witness interviews

See Chapter 23 on negotiating global settlements

In particular, close coordination is necessary between the company's criminal and civil legal advisers to ensure consistency of approach.

Privilege waivers and disclosure obligations 33.8.2

During the course of an investigation, documents which attract privilege may be shown or provided to relevant authorities, often to demonstrate co-operation. These include not only privileged communications between lawyer and client but also documents, such as witness interview notes, generated by external counsel. Doing so will not necessarily constitute a general waiver of any privilege in those documents for the purposes of subsequent civil proceedings (particularly if it is made clear that this is done on a limited basis), although it may lead to adverse consequences, as the company will lose a degree of control over the information in the documents. However, care should be taken in cases involving multiple jurisdictions, as the effect of showing or providing a potentially privileged document to the authorities may vary depending upon which law governs questions of privilege.

Concurrent settlements 33.9

Difficult issues can arise for companies when attempting to negotiate settlement of global investigations, which can involve a variety of regulatory and prosecuting authorities across a range of jurisdictions. Parallel existing (or potential) civil litigation or arbitration adds a further layer of complexity to the analysis.

See Chapter 23 on negotiating global settlements

During settlement negotiations with the authorities, companies should be aware of the risk that the fact of a settlement, as well as any associated press coverage or documents (such as a statement of facts in a DPA), may raise awareness of potential civil claims, and in certain circumstances may even be relied upon to support such claims. This will be of particular concern in the competition law context, given the risk of follow-on actions. (Notably, the European Commission's settlement procedure for cartel cases requires parties to acknowledge liability for an infringement.) Accordingly, and to the extent possible, companies should avoid admitting liability as part of any negotiated settlement with the authorities; and, if an admission of liability is required, they should ensure that it is tightly circumscribed.

See Section 33.7

See Chapter 23 on negotiating global settlements and Chapter 35 on privilege

In addition, there is a risk that communications with the authorities made during the course of settlement negotiations will be disclosable in subsequent civil proceedings, although they may be protected from inspection by a right analogous to the 'without prejudice' rule.

See Chapter 23 on negotiating global settlements

Settlement of civil claims can also carry risks for a company under investigation. There is a risk that settlement agreements entered into by the company may be disclosable in subsequent proceedings, or requested by an authority as part of their investigations. Companies should avoid admitting liability as part of any negotiated civil settlement. In addition, authorities may perceive certain types of civil settlements (particularly those with witnesses for substantial sums) as suspicious.

In appropriate circumstances, it may be possible to settle civil claims on a multi-party basis. For instance, companies may try to reach collective settlements, which are available in respect of certain competition law claims (using the mechanism set out in the Competition Act 1998), or seek to utilise a collective redress scheme.

33.10 Concluding remarks

Cross-border investigations are complex and competing considerations need to be carefully weighed and managed. The prospect of parallel civil proceedings brings further complexity to an already difficult area. Such proceedings can present numerous and diverse challenges for a company subject to investigation – it may face a range of different types of action, on a number of fronts (for instance, involving shareholders, suppliers, customers or employees), which may impact an investigation, or be affected by an investigation, in a variety of ways. Companies will frequently be defendants in parallel proceedings and unable to exercise significant control over the existence or pace of the proceedings. They may at times be claimants out of necessity or to obtain a tactical advantage. It is important to give careful consideration at an early stage to potential parallel proceedings which may arise, and any effect they may have on an investigation (and *vice versa*), to enable possible tensions between investigations and parallel proceedings to be anticipated and managed effectively. There is no easy solution to the challenges presented by parallel civil proceedings. As noted above, it may be difficult to obtain a stay of them (without the consent of other parties to the proceedings), and settlements can give rise to their own particular complications.

34

Parallel Civil Litigation: The US Perspective

Eugene Ingoglia and Anthony M Mansfield[1]

Introduction 34.1

In the United States, criminal and regulatory investigations often generate parallel civil proceedings. Such proceedings often take the form of class actions, in which a lead plaintiff seeks to prosecute claims on behalf of a large number of similarly situated plaintiffs who allege damage resulting from the conduct under investigation. Plaintiffs may also attempt to bring suits against alleged wrongdoers, such as corporate officers and directors, derivatively on behalf of a company.

Civil proceedings that are generated in connection with an investigation can precede the investigation, follow on from investigative findings or, frequently, arise during the course of the investigation. Public disclosures by a company about the existence or results of a criminal or regulatory investigation and other similar publicly available corporate announcements frequently give rise to civil claims relating to the conduct at issue. Civil proceedings can also bring about investigations in circumstances, for example, where a civil suit challenges conduct that was unknown to the relevant authorities.

It can be challenging to manage parallel civil proceedings that are governed by their own procedural rules and can interfere with the pacing of an investigation or create other tensions with the investigative process. This chapter addresses issues in parallel proceedings that may arise in connection with complex investigations. Similar considerations may apply when dealing with a criminal investigation and parallel civil enforcement proceedings brought by regulatory agencies such as the Securities and Exchange Commission or the Commodity Futures Trading Commission.

1 Eugene Ingoglia and Anthony M Mansfield are partners at Allen & Overy LLP.

34.2 Stay of proceedings

When a company under investigation is also involved in ongoing civil proceedings (before a court or an arbitral tribunal) that relate to the conduct under investigation, a party or the government may seek to stay those proceedings pending the outcome of the investigation. While this is often desirable to avoid tension between a civil litigation and an investigation, it is difficult to achieve. A court's decision to grant a stay is, as a general matter, entirely discretionary.[2]

While courts in the US are sensitive to the potential prejudice to an individual or entity under investigation that is forced to proceed with civil litigation about the same conduct, and in particular the potential that an individual's constitutional right against self-incrimination may be compromised,[3] courts are nevertheless hesitant to stay civil cases simply because an investigation is pending. If a stay is granted, a court may impose conditions and limitations, including limitations on length. A stay of civil proceedings will freeze the proceedings until the stay expires or the court issues a further order. A party can apply to have a stay lifted at any time.

In criminal investigations or proceedings, the government may seek a stay to protect the criminal process, including limiting a company's ability to use civil litigation to obtain broader discovery than is available in a criminal case. For instance, in a parallel civil case, putative or actual defendants in the related criminal proceedings can seek the deposition testimony in the civil case of key witnesses that the government intends to rely on in the criminal case, providing a significant advantage to defendants that would not otherwise exist in the absence of the civil case. Courts have discretion to impose full or partial stays of the civil proceedings.

34.3 Class actions

In the United States, class actions are a centrepiece of complex civil litigation, particularly in securities and antitrust litigation, as the misconduct alleged often impacts large markets and large numbers of entities and individuals. More often than not, a complex criminal or regulatory investigation will generate class action litigation.

34.3.1 Background

In the United States, class actions may be brought on behalf of similarly situated claimants. There are many scenarios in which class actions may be certified, but class actions typically involve cases where there are a significant number of

2 See *Twenty First Century Corp. v. LaBianca*, 801 F. Supp. 1007, 1010 (E.D.N.Y. 1992) (citing *Kashi v. Gratsos*, 790 F.2d 1050, 1057 (2d Cir. 1986)). Courts balance a number of factors in determining whether to grant a stay, including '(1) the private interest of the plaintiffs in proceeding expeditiously with the civil litigation as balanced against the prejudice to the plaintiffs if delayed; (2) the private interests of and burden on the defendant; (3) the convenience to the courts; (4) the interest of persons not parties to the civil litigation; and (5) the public interest.' Id. (internal quotations and citation omitted).

3 Corporations do not enjoy the constitutional privilege against self-incrimination.

claimants and common legal issues predominate over any individualised issues, so that the litigation can fairly be prosecuted on a representative basis. A class action is litigated similarly to an individual action, except that the plaintiff must file a motion asking the court to certify the class, and there may be litigation about which plaintiff will be lead plaintiff in the action.[4] The defendant may oppose class certification on many grounds, including that too many individualised issues exist. Motions for class certification are moving to the later stage of cases, and, unless the motion for class certification is denied, the case will proceed on a class basis, with a representative plaintiff leading.

Class actions following release of reports, findings, etc. 34.3.2

In the United States, class actions against a company arise frequently following the release of internal investigation reports, regulatory findings or entry into a deferred prosecution agreement with the government, as these documents can provide a road map for a civil plaintiff's claims and are frequently cited in class action complaints as support for the plaintiff's allegations. When such documents become available publicly, the risk is quite high that one or more civil class actions will follow. If a class action survives a motion to dismiss based on threshold legal infirmities or pleading deficiencies and proceeds to discovery, a class action plaintiff will frequently demand that the company produce all materials that have been provided to the government, in addition to other disclosure requests under broad US discovery requirements.

The release of such internal investigation reports, regulatory findings or a deferred prosecution or plea agreement may also cause potential class action plaintiffs to seek documents a company has provided to the government in connection with an investigation directly from the government through a Freedom of Information Act (FOIA) request.[5] Indeed, a FOIA claim could be pursued even before internal investigation reports, regulatory findings or a deferred prosecution agreement become public, provided a claimant has a basis to make a request.

As a general matter, FOIA allows members of the public to access records from any federal agency. Most states have equivalent laws.[6] FOIA is subject to a number of exemptions, which should be considered any time a FOIA request is directed to company information in the government's possession. These exemptions, while narrowly construed, include certain exemptions for records or information compiled for law enforcement purposes as well as exemptions for documents relating to reports prepared by, on behalf of or for the use of agencies that regulate financial institutions. It is therefore rare for FOIA requests to be granted during an investigation. Production of documents to government entities typically is accompanied

4 Fed. R. Civ. P. 23(c).

5 FOIA, which is codified at 5 U.S.C. § 552, is a law that allows members of the public to seek access to information in the possession of the government.

6 'State law' in this chapter refers to New York law unless otherwise noted. This chapter does not purport to address the potential variances in the laws of all 50 US states.

by a request for FOIA exemption.[7] In practice, prosecuting an FOIA claim can be a slow and cumbersome process.[8]

34.3.3 Process

Federal class actions are governed by Rule 23 of the Federal Rules of Civil Procedure. Before a judgment in a class action can issue, a class must be certified. Because of the high standard for class certification and the evidentiary support required, class certification motions are typically filed at the conclusion of the discovery phase. Class certification is often hotly contested. To achieve certification, the proponent of class status must show that the class is so numerous that joinder of all members is impracticable, there are common questions of law or fact, the claims of the proposed representative of the class are typical of the claims of the class as a whole and the proposed representative will adequately represent the interests of the class.[9]

Once these criteria are satisfied, the action must fit into one of three categories: (1) suits where separate actions might cause a risk of inconsistent judgments or where assets available to pay claims are limited; (2) suits seeking injunctive relief where any monetary remedy would be only incidental to the injunctive relief; and (3) suits seeking money damages.[10] Most cases fall within the third category. For these cases, in addition to the criteria set forth above, the proponent of class status must show that the common questions of fact or law predominate, and that class treatment is the superior method for adjudication.[11]

Other than the certification phase, the case proceeds as would an ordinary civil litigation. Typically, this will involve a motion to dismiss at the pleadings stage seeking to end the case based on legal infirmities or at least narrow the claims and issues in dispute. If any claims survive, the parties will proceed to discovery, which involves the exchange of typically voluminous documents and the deposition testimony of witnesses under oath. Witnesses who may be implicated in misconduct may refuse to testify on the grounds that doing so would infringe their constitutional right against self-incrimination.[12]

---

7 See 17 C.F.R. § 200.83 for a description of confidential treatment procedures under FOIA.

8 Designation of information as confidential under FOIA does not necessarily render the information unavailable for purposes of discovery in civil litigation. See, e.g., *Friedman v. Bache Halsey Stuart Shields, Inc.*, 738 F.2d 1336, 1344 (D.C. Cir. 2009) ('[I]nformation unavailable under the FOIA is not necessarily unavailable through discovery.'); see also *In re Subpoena Duces Tecum*, 439 F.3d 740, 753-54 (D.C. Cir. 2006). ('FOIA's exceptions to disclosure limit only the right to information conveyed pursuant to that statute and other limitations on the Commission's authority to publish information . . . do not alter the Commission's duty to comply with lawful subpoenas after notice to the party whose information is sought.') (Citations omitted.)

9 Fed. R. Civ. P. 23(a).

10 Fed. R. Civ. P. 23(b).

11 Id.

12 U.S. Const. amend. V.

Discovery is typically followed by motions for summary judgment based on a lack of material facts in dispute.[13] If the motion for summary judgment fails, the case proceeds to trial. Settlement of federal class actions must be approved by the court, and must be on notice to all potential class members, who are given the opportunity to opt out of the settlement. If a class was not certified prior to settlement, a streamlined class certification motion is filed in connection with seeking approval of the settlement. Settlement agreements often provide a settling defendant the right to back out if too many class members opt out of the class.

Class Action Fairness Act of 2005 34.3.4

The Class Action Fairness Act of 2005 (CAFA) greatly expanded the federal courts' jurisdiction over class actions by relaxing the requirements for federal subject matter jurisdiction.[14] This allows defendants to remove class actions from state courts to federal courts, and to consolidate multiple state proceedings into a single federal court class action. As federal courts generally have more experience of administering class actions than state courts, this outcome is often seen as desirable.

CAFA requires courts to scrutinise class action settlements involving corporations more closely. CAFA also requires notice of settlements to be provided to state attorneys general so they may intervene to protect citizens who are class members.

Securities class actions: PSLRA & SLUSA 34.3.5

There are two statutory schemes applicable in securities class actions aimed at curtailing frivolous securities lawsuits: the Private Securities Litigation Reform Act of 1995 (PSLRA)[15] and the Securities Litigation Uniform Standards Act of 1998 (SLUSA).[16]

Among other changes to the securities litigation landscape, the PSLRA makes it more difficult for a plaintiff to plead securities fraud by requiring the plaintiff to plead false statements with particularity, establish a strong inference that each defendant knew the statements alleged were false when made, and allege loss causation. In addition, and importantly from a defendant's perspective, the PSLRA stays discovery until the court has determined, usually following a motion to dismiss, whether a claim for securities fraud has been adequately stated.

SLUSA was enacted to combat efforts by plaintiffs to avoid the strictures of the PSLRA by pursuing state law claims, such as common law fraud, through class actions in state courts. Broadly speaking, SLUSA bars claims, whether filed in state or federal court, that allege fraud under state law in connection with the

13 Fed. R. Civ. P. 56(a). ('The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.')

14 28 U.S.C. §§ 1332(d) et seq.

15 15 U.S.C. §§ 78u-4, 78u-5 et seq.

16 15 U.S.C. §§ 77p, 78bb et seq.

purchase or sale of securities from being pursued in a class action.[17] SLUSA can be a powerful tool in limiting the scope of claims in a securities class action at the outset.

34.3.6 Other considerations: class action waivers in arbitration agreements

In recent years, the United States Supreme Court has held that class action waivers in arbitration agreements are enforceable under the Federal Arbitration Act (FAA).[18] Thus, companies should consider subjecting claims by counterparties, customers or employees to arbitration and should include class action waivers in the arbitration agreement. Arbitration agreements typically provide that proceedings will be confidential, and in the absence of access to the class action device, a claimant with meritless claims or claims with low monetary value may be less inclined to pursue them.

34.4 Derivative actions

34.4.1 Law and procedure

In general, under state law, members or shareholders of a company can bring a derivative claim alleging harm to a company and seeking relief on its behalf.[19] Before bringing a claim, a plaintiff must generally show that it has made a demand on the company to bring the claim in its own name and the company has refused to do so, or that making such a demand would be futile.[20] The plaintiff must name the company as a nominal defendant in the suit, and the company will thereby have the right to participate. Recovery in a derivative action flows to the company.

34.4.2 Practical considerations: indemnification of officers and directors

Typically derivative claims are brought by minority shareholders against majority shareholders or corporate officers and directors. Corporate officers and directors are often entitled to indemnification by the company for such suits pursuant to a company's by-laws, subject to any requirements or restrictions that may

17 There is an important exception to this general rule. The United States Supreme Court recently held that SLUSA does not prohibit state court class actions arising from a company's initial public offering, which is governed by the 1933 Securities Act, as distinct from a company's subsequent offerings, which are governed by the 1934 Securities and Exchange Act, and are covered by SLUSA. See *Cyan Inc. v. Beaver Cnty. Employees Retirement Fund*, 138 S. Ct. 1061 (2018).

18 See *DirecTV v. Imburgia*, 136 S. Ct. 463 (2015); see also *AT&T Mobility v. Concepcion*, 563 U.S. 333 (2011). See also *Epic Sys. Corp. v. Lewis*, 138 S. Ct. 1612 (2018) (holding that arbitration agreements providing for individualised employee proceedings against employers must be enforced, notwithstanding provisions in statutory schemes to promote collective employment actions by employees). The Federal Arbitration Act is codified at 9 U.S.C. §§ 1 et seq.

19 See, e.g., N.Y. Bus. Corp. L. § 626 (authorising shareholder derivative suits).

20 When such a demand is made, companies sometimes form a 'special litigation committee' or 'demand review committee' consisting of disinterested and independent directors to determine whether pursuing the claim proposed by the shareholder is in the company's best interests. A special litigation committee's determination that such a claim should not be brought can provide a strong defence to defendants in a shareholder derivative action.

be imposed by state law,[21] and this is therefore an important consideration at the outset of any derivative suit. Ordinarily, officers and directors cannot claim indemnification for bad faith conduct, so where a company's board of directors determines that bad faith conduct has occurred – which determination is highly likely if criminal acts or regulatory misconduct are admitted by officers and directors, such as through a guilty plea – the question of indemnification becomes complicated and often requires careful parsing of whether the amounts claimed are subject to indemnification notwithstanding admission of unlawful acts. The outcome will depend both on the statutory scheme in the state whose laws govern the relationship between the director or officer and the company, as well as the breadth of corporate reimbursement provisions of the relevant insurance policy. Where a determination of whether the conduct at issue rose to the level of bad faith has not yet been reached, officers and directors often have the right to have their legal costs advanced by the company, pending such determination.

Other private litigation 34.5

Opt-out claims 34.5.1

Individuals who may be class members in a class action may opt out of participation in the class and pursue claims individually, which can result in a company having to litigate duplicative claims in multiple jurisdictions. To avoid a significant number of opt-outs, a company can attempt to achieve a class action settlement with terms attractive to class members.

Purchaser claims 34.5.2

Purchasers of securities of a company under investigation may, once the investigation comes to light, claim that they were defrauded into purchasing securities by material misstatements made by the company while it knew the investigation was pending. Such claims can be brought on an individual or class basis, subject to the limitations of the PSLRA and SLUSA.

Negative impact on contract enforcement rights 34.5.3

Conduct that is illegal or contrary to public policy (and which may, therefore, also be the subject of an investigation or litigation) may render related contracts entered into by a company void or voidable.

The common law doctrine of illegality prevents a party to a contract from enforcing its contractual rights and remedies in certain circumstances, where the contract is tainted by conduct that is illegal, or contrary to public policy (some contracts may also be rendered unenforceable by statute). The law in this area is highly dependent on facts and circumstances, and courts weigh a variety of factors in determining whether to enforce the provisions of an illegal contract.[22]

21 See, e.g., N.Y. Bus. Corp. L. § 722 (authorising indemnification of corporate officers and directors); 8 Del. C. § 145 (same).

22 See, e.g., *Denburg v. Parker Chapin Flattau & Kimpl*, 82 N.Y.2d 375, 385 (1993).

34.5.4 Specific provisions in commercial contracts

Parties often include specific provisions in their commercial contracts (including finance documents) aimed at preventing, or providing contractual protection in relation to, illegal behaviour (e.g., corruption) involving a party to the agreement. Accordingly, the fact of an investigation (or related proceedings), or conduct that is the subject of an investigation, may have adverse contractual consequences for a company. Such consequences will depend on both the investigation and the specific conduct under investigation, as well as the contractual provisions. Such provisions may include:

- obligations:
  - to comply with certain applicable laws and regulations;
  - to have in place and comply with specified policies (such as anti-bribery and corruption policies);
  - to maintain accurate records of payments made in relation to the contract;
  - in relation to subcontractors (for instance, to ensure that subcontractors comply with requirements equivalent to those imposed on the company), and that may impose responsibility on the company for any non-compliance by a subcontractor with such requirements;
  - to report generally on compliance to counterparties on an ongoing basis, which could include requiring the provision of a confirmation signed by an officer of the company or audit rights; and
  - to report the occurrence of certain events to counterparties. These could include dealing with a public official in connection with the performance of the contract, receiving a request for a payment (or other advantage) in connection with the performance of the contract, or the commencement (or threat) of an investigation into the activities of the company;
- representations (given by the company, and which may be repeated) that it has not been investigated for or convicted of certain offences (and that no proceedings or investigations are pending or threatened), or which relate to the accuracy and completeness of information provided to contractual counterparties;
- termination rights for counterparties if the company breaches (or, potentially, if the counterparty reasonably suspects a breach of) certain obligations, or if the company makes a false representation or is convicted of certain offences; and
- indemnities (for the benefit of counterparties) in respect of loss suffered as a result of a certain breaches of the contract by the company.[23]

A company may face parallel litigation brought by its contractual counterparties in reliance on such provisions. A company may also be able to invoke such provisions against its counterparties, although where a company is under investigation, it may be barred from taking the position in civil proceedings that its counterparty has engaged in illegal activity if the company is also exposed for its counterparty's

23 An indemnity against a criminal liability may, however, be unenforceable for public policy reasons.

conduct, as the company would be *in pari delicto* or, in other words, equally guilty such that the court will refuse to intercede in a dispute between them.[24]

Mergers, acquisitions and investments 34.5.5

Mergers, acquisitions and investments can present particular risks for companies. Illegal behaviour in the target company (or its subsidiaries, or other related companies and persons) may have various negative consequences for an acquiring entity, which can include financial consequences (for example, the target may have been overvalued); legal consequences (both civil and criminal) for the target, the acquiring entity and relevant individuals (including officers of both entities),[25] along with associated legal costs; and other practical consequences (for example, reputational damage, which may have a consequent effect on business).[26]

As a result, acquiring entities will often take precautions to minimise these risks. Typically, these include conducting proportionate pre- and post-acquisition due diligence of the target and its business, including without limitation review of all of the target's business dealings and third-party contracts, implementing compliance programmes and including appropriate protections in the relevant contractual documentation.

In relation to the latter, warranties, representations and indemnities[27] designed to provide such protection are frequently included in share purchase agreements. The scope of protection will depend on the particular provisions negotiated, but they can be widely drafted, such that they encompass the conduct of, for example:

- the target and its subsidiaries;
- directors, officers, employees, significant shareholders, affiliates, agents, and distributors of the target and its subsidiaries;
- those associated with or acting on behalf of the target and its subsidiaries; and
- those who perform services for or on behalf of the target and its subsidiaries,

24 See *Kirschner v. KPMG LLC*, 15 N.Y.3d 446 (2010).

25 The Department of Justice (DOJ) recently issued an opinion addressing factors that may be relevant in determining whether and how the DOJ would seek to impose post-acquisition successor liability on an acquirer for pre-acquisition Foreign Corrupt Practices Act (FCPA) violations by its target. See US Department of Justice, Foreign Corrupt Practices Act Review, No. 14-02 (7 November 2014). The DOJ 'encourages companies engaging in mergers and acquisitions to (1) conduct thorough risk-based FCPA and anti-corruption due diligence; (2) implement the acquiring company's code of conduct and anti-corruption policies as quickly as practicable; (3) conduct FCPA and other relevant training for the acquired entity's directors and employees, as well as third-party agents and partners; (4) conduct an FCPA-specific audit of the acquired entity as quickly as practicable; and (5) disclose to the Department any corrupt payments discovered during the due diligence process.' Id. at 3-4.

26 Companies should also be aware of the risk that illegal behaviour (for example, bribery) may occur during the merger, acquisition or investment transaction.

27 However, see footnote 23 above in relation to indemnities against criminal liability.

and may cover areas such as:

- compliance with laws generally;
- compliance with anti-money laundering laws and standards;
- compliance with anti-bribery and corruption laws and standards;
- debarment from public contracts;
- sanctions (including whether such persons are, have been, or are likely to become, subject to sanctions); and
- whether such persons are (or have been) subject to an investigation or any proceedings, or whether an investigation or any proceedings in respect of such persons are pending, threatened, contemplated or even likely.

Accordingly, the fact of an investigation (or related proceedings), or conduct which is the subject of an investigation, may give the acquiring entity contractual rights it can seek to enforce (including through litigation or arbitration). The acquiring entity should, therefore, review all of the target's business dealings and third-party contracts for potential exposure, which may include consideration of the target's in-house and external legal advice relating to such dealings and contracts.[28] Again, however, care may need to be taken in doing so for the reasons given at Section 34.5.4.

34.5.6 Employment law, defamation and whistleblowing

Investigations can have employment law consequences for a company. Employees may seek to bring claims against their employers arising out of the subject matter of an investigation, or how the investigation is handled; conversely, an employer may wish to take action against an employee implicated in the conduct under investigation. Employees may also pursue claims for defamation based on statements a company may make about their conduct either internally or to the government.[29]

See Chapter 14 on employee rights

In addition, to the extent that allegations have been made by whistleblowers, companies under investigation or conducting investigations should be careful to respect whistleblower rights to avoid claims for breach of the protections afforded to whistleblowers.

See Chapter 20 on whistleblowers

28 An acquiring company should be conscious, however, of the potential for a privilege waiver by the target company if such legal advice is shared outside the context of litigation. The law on this subject varies from state to state, but in New York, for example, pre-closing communications between counsel for a target company and its acquirer are not privileged unless they relate to pending or anticipated litigation. See *Ambac Assurance Corp. v. Countrywide Home Loans, Inc.*, 27 N.Y.3d 616 (2016).

29 See, e.g., *Mott v. Anheuser-Busch, Inc.*, 910 F. Supp. 868, 874-78 (N.D.N.Y. 1995) (granting summary judgment in favour of employer on employee defamation claim stemming from employer's investigation and subsequent reporting of employee's illegal conduct, and finding that the investigation was conducted in a 'thorough and responsible manner' because it was initiated immediately following reports of wrongdoing, included interviews with all relevant parties and an extensive review of books and records, and was undertaken by a team including both inside and external counsel).

Evidentiary issues 34.6

Reliance by the court on statements of facts in authority findings 34.6.1

Parties will often seek to rely on findings made by the government as the result of an investigation in subsequent civil litigation. To the extent facts are admitted in, for example, a deferred prosecution agreement or a guilty plea, those facts will generally be admitted into evidence as party admissions under US evidentiary rules.[30] Deferred prosecution agreements may also specifically prohibit a company from denying certain facts. In addition, to the extent a party discloses otherwise privileged information to the government in connection with a deferred prosecution or plea agreement, there may be a privilege waiver by that party in any related civil litigation.

Reliance by the authority on findings of a court 34.6.2

Conversely, facts discovered during the course of civil litigation may draw the attention of the government, and the government may rely on the findings in a civil case as grounds for opening an investigation or taking some other enforcement action. Accordingly, these risks may be relevant considerations for a company when considering and implementing its litigation strategy in civil proceedings. In addition, conflicted representation and privilege issues may arise if the interests of the company and its employees are not aligned. For example, company counsel may represent a key employee witness at deposition in a civil case, but in the context of a subsequent criminal investigation may be conflicted from continuing the representation should the employee's interests diverge from the company's interests,[31] such as where the company wishes to disclose misconduct to the government but the employee wishes to invoke his or her Fifth Amendment privilege against self-incrimination.

30 A settlement with a civil regulator may be reached without the company (or the individual) admitting or denying the regulator's findings set forth in the settlement order. In this circumstance, the regulator's findings are generally inadmissible in subsequent civil litigation. See, e.g., *Wilson v. Parisi*, 2009 U.S. Dist. LEXIS 3970, at *6-7 (M.D. Pa. 21 January 2009) (excluding consent decrees under Federal Rule of Evidence 408); see also *Bowers v. NCAA*, 563 F. Supp. 2d 508, 536 (D.N.J. 2008) (holding Rule 408 'plainly applicable' to the consent decree at issue and refusing to allow the plaintiff to use a consent decree between the defendant and the Department of Justice as evidence of the defendant's liability for the conduct underlying the plaintiff's claim); *Carpenters Health & Welfare Fund v. Coca-Cola Co.*, 2008 U.S. Dist. LEXIS 112503, at *22 (N.D. Ga. 23 April 2008) (granting motion to exclude SEC civil consent order from evidence); *In re Blech Sec. Litig.*, 2003 U.S. Dist. LEXIS 4650, at *25-30 (S.D.N.Y. 26 March 2003) (finding SEC consent judgments inadmissible under Rule 408); *Safford v. St. Tammany Parish Fire Prot. Dist. No. 1*, 2003 U.S. Dist. LEXIS 6513, at *16 (E.D. La. 11 April 2003) (holding that consent decree cannot be used as evidence of prior liability).

31 See, e.g., N.Y. Unified Court System, Rules of Professional Conduct, Rule 1.7(a)(1) (a lawyer cannot concurrently represent two clients with differing interests).

34.6.3 Collateral use of disclosed documents

In the United States, the scope of discovery in civil cases is very broad, and parties in federal civil litigation must typically disclose all potentially relevant non-privileged evidence.[32] Confidentiality of a relevant document is not a justification for refusing to disclose it, though confidential documents are often protected from public disclosure by protective orders.

As a result, a company involved in civil proceedings may be required to disclose sensitive documents to an opponent, including documents relevant to an investigation or even unprivileged investigation material. Where an adversary is aware of an investigation, it will typically demand production of any document that has been given to the government, and in practice, apart from privileged documents, such documents are produced. In making a production to an adversary, a company should seek a protective order that requires the adversary to maintain the information as confidential, refrain from using the information for any purpose other than litigation, seek to have the information filed under seal when reference to the information is made in court filings, and destroy the information at the conclusion of litigation.

34.7 Practical considerations

34.7.1 Coordination with internal investigations team

It is important that those within the company responsible for managing parallel civil litigation are in constant communication with the internal team responsible for dealing with investigations, to ensure that:

- a clear, holistic strategy is developed for managing the investigations and parallel civil proceedings, and anticipating areas of potential risk (e.g., civil claims that may arise, but have not yet been commenced);
- both teams understand, and evaluate the risks of, new developments in both the criminal and civil context; and
- any proposed action by the company or associated persons, in the civil or criminal context, is carefully analysed to determine the potential repercussions for all other proceedings and investigations.

Issues can arise, for instance, where:

- factual admissions are made in civil proceedings (such as in an answer or in interrogatory responses) that may undermine the defence of the criminal case;
- an authority seeks disclosure of privileged documents from the company in circumstances where the company may wish to assert privilege over those documents in subsequent civil proceedings;
- witnesses, whose testimony may be important for the company's case in civil proceedings, are under investigation, or have been classified as suspects, by the authorities, and have concerns about self-incrimination. Depending on the

See Chapter 8 on witness interviews

32 Fed. R. Civ. P. 26(b)(1).

circumstances, employment proceedings may also be ongoing in respect of such individuals;
- pleading possible defences (such as illegality) in civil proceedings, which may strengthen the company's case in those proceedings but would undermine the position it has taken in relation to an investigation; or
- as part of deferred prosecution agreement negotiations, there is a risk that matters an authority seeks to include in an agreed statement of facts could be relied on against the company in parallel civil proceedings.

In particular, close coordination is necessary between the company's criminal and civil legal advisers to ensure consistency of approach.

Privilege waiver and disclosure obligations 34.7.2

During an investigation, documents entitled to privilege or work-product protection may be shown or provided to relevant authorities, often to demonstrate co-operation. These include not only privileged communications between attorney and client but also documents, such as witness interview notes, generated by external counsel. Depending on the applicable privilege law, which can vary widely from state to state and even among the federal circuit courts of appeal, sharing such information will not necessarily constitute a general privilege waiver for the purposes of subsequent civil proceedings (particularly if it is made clear that this is done on a limited basis), although it may lead to adverse consequences, as the company will lose a degree of control over the information in the documents.[33] In cases involving multiple jurisdictions, it is critical for a company to obtain advice on all potentially applicable privilege laws prior to showing potentially privileged documents to the government, as the effect of showing or providing a potentially privileged document to the authorities may vary depending on which law governs questions of privilege.

Concurrent settlements 34.8

Difficult issues can arise for companies when attempting to negotiate settlement of global investigations, which can involve a variety of regulatory and prosecuting authorities across a range of different jurisdictions. Parallel existing (or potential) civil litigation or arbitration adds a further layer of complexity to the analysis.

See Chapter 24 on negotiating global settlements

During settlement negotiations with the authorities, companies should be aware of the risk that a settlement, as well as any associated press coverage or documents (such as a statement of facts in a deferred prosecution agreement), may raise awareness of potential civil claims, and in the class action context will likely be relied on to support claims. Documents pertaining to the negotiation of a settlement, including communications with the relevant authority and drafts

33 As a condition for the disclosure of otherwise privileged information, a regulator may stipulate that it will not assert a waiver of applicable privilege in any subsequent enforcement action. However, a stipulation by a regulator does not bind third parties.

of the settlement, may be discoverable by plaintiffs in any such civil action.[34] Accordingly, and to the extent possible, companies should avoid admitting liability as part of any negotiated settlement with the government; and, if an admission of liability is required, they should ensure that it is narrowly circumscribed. Companies should further consider what they convey during the course of settlement discussions and how they communicate such information.

See Chapter 24 on negotiating global settlements

Settlement of civil claims can also carry risks for a company under investigation, in particular class action settlements, which are public. Companies should avoid admitting liability as part of any negotiated civil settlement. In addition, the government may perceive certain types of civil settlements (particularly settlements with potential witnesses for substantial sums) as suspect.

34 Federal Rule of Evidence 408 limits the admissibility of evidence pertaining to settlements and their negotiation. It does not, however, speak to the discoverability of such information. Numerous courts have addressed the availability of a 'settlement privilege' to limit discovery of settlement related documents, reaching different conclusions. Compare *Stockman v. Oakcrest Dental Center P.C.,* 480 F.3d 791 (6th Cir. 2007) (applying settlement privilege), with *Morse/Diesel, Inc. v. Fidelity & Deposit Co. of Maryland*, 122 F.R.D. 447, 449 (S.D.N.Y. 1988) (declining to recognise settlement privilege).

35

Privilege: The UK Perspective

Tamara Oppenheimer, Rebecca Loveridge and Samuel Rabinowitz[1]

Introduction 35.1

The law of privilege confers on persons the right to refuse to produce a document or to answer questions – including by a regulator or prosecuting authority. The two subcategories of legal professional privilege are (1) legal advice privilege and (2) litigation privilege. This chapter explains the basic principles applicable to these, having particular regard to the regulatory and investigatory context. It also addresses briefly two other types of privilege that may arise in the regulatory context, namely common interest privilege[2] and without prejudice privilege.

This chapter also discusses certain exceptions to privilege and the circumstances in which privilege can be lost or 'waived', either intentionally or inadvertently. The final section of the chapter addresses some more practical issues of how to maintain privilege in the regulatory and investigatory context.

1 Tamara Oppenheimer, Rebecca Loveridge and Samuel Rabinowitz are members of Fountain Court Chambers. The authors are grateful to Bankim Thanki QC for his contributions to previous editions of this chapter.

2 Common interest privilege (as with joint interest privilege) is traditionally analysed as a distinct category of privilege, although it depends on the existence of material to which either legal advice or litigation privilege applies.

35.2 Legal professional privilege: general principles

The relevant distinction between legal advice privilege and litigation privilege is as follows:[3]

- Legal advice privilege is concerned with communications between lawyer and client for the purpose of giving or receiving legal advice or assistance,[4] in both the litigation and the non-litigious context.
- Litigation privilege is concerned with communications between a client or his or her lawyer and third parties for the purposes of litigation (whether anticipated or commenced).

Notwithstanding frequent misconceptions to the contrary, litigation privilege has no application to communications between lawyer and client, even where litigation is anticipated or has actually commenced: such communications will always fall within the ambit of legal advice privilege.[5]

Before turning to consider these two aspects of legal professional privilege separately, a number of general observations should be made.

35.2.1 The need for confidentiality

Privilege requires and protects the confidentiality of documents and exchanges. Confidentiality is therefore a necessary, but not a sufficient, condition for both limbs of legal professional privilege.[6] The question is whether a document has the necessary quality of confidence, such as to attract privilege. This is rarely problematic, as it can usually be inferred that communications between lawyers and their clients or with third parties in the context of actual or anticipated litigation have been impressed with confidence. Nevertheless, some communications may be regarded as lacking that character. Hence, in the context of legal advice privilege, the client's identity,[7] address[8] or the existence of the retainer[9] will not generally be deemed to be confidential (or, accordingly, privileged). While a lawyer will usually

3 *Waugh v. British Railways Board* [1980] AC 521, 541-542, HL (*per* Lord Edmund-Davies). The distinction set out in Lord Edmund-Davies' speech was applied by the Court of Appeal in *Re Highgrade Traders Ltd* [1984] BCLC 151, 164, 165 (*per* Oliver LJ); and by the House of Lords in *In re L (a Minor) (Police Investigation: Privilege)* [1997] AC 16, 24-5 (*per* Lord Jauncey) and *Three Rivers District Council and others v. Governor and Company of the Bank of England (No. 6)* [2005] 1 AC 610, HL (*Three Rivers No. 6*), para. 65 (*per* Lord Carswell) and paras. 50, 51 (*per* Lord Rodger).

4 See *Thanki* (ed.), *The Law of Privilege* (3rd edn.), para. 2.02.

5 See *Thanki*, paras. 1.09-1.12; Passmore, *Privilege* (3rd edn.), paras. 3.002 to 3.005.

6 *Three Rivers No. 6*, para. 24 (*per* Lord Scott).

7 *Bursill v. Tanner* (1885) 16 QBD 1, 4; *Pascall v. Galinski* [1970] 1 QB 38; *R (Miller Gardner) v. Minshull St Crown Court* [2002] EWHC 3077 (Admin); *R (Howe) v. South Durham Magistrates Court* [2005] RTR 4. See generally A Pugh-Thomas, 'Who is your client?' (1997) SJ 141(2) 44.

8 *Ex Parte Campbell* (1869-70) LR 5 Ch App 703, 705. However, in this case James LJ made clear that the position may be different if the client's residence has been told to the lawyer as a matter of professional confidence. These *dicta* were applied in *Re Arnott, ex p Chief Official Receiver* (1888) 60 LT 109.

9 *Levy v. Pope* (1829) M & M 410; *Gillard v. Bates* (1840) 6 M & W 547.

owe his or her client enforceable duties of confidence,[10] for the purposes of litigation privilege, communications between a lawyer or client and a third party do not have to be 'confidential' in the sense that the third party is bound by equitable (or contractual) duties of confidence not to reveal the communication to anyone else.[11] In the context of litigation privilege, the requirement of confidentiality is therefore perhaps best put in terms of the communication or other document being 'not properly available for use'.[12]

Legal professional privilege as a substantive right 35.2.2

Legal professional privilege is not merely an exclusionary rule of evidence, but is also a substantive right, which is afforded overriding importance within English law.[13] The House of Lords and the Supreme Court have repeatedly emphasised its importance and its role in the administration of justice. It has been characterised as both 'a fundamental human right'[14] and 'a fundamental condition on which the administration of justice as a whole rests'.[15]

If it were simply a rule of evidence, a client could only prevent disclosure in legal proceedings. There would be no guarantee that the same material could be kept from the police or some other agency, such as a financial regulator or prosecuting authority, with the power to compel the production of documents or information. Hence, legal professional privilege can now generally be asserted in answer to any demand for documents by a public or other authority; it is not limited to a right that may be asserted only in the context of civil or criminal proceedings.

It is, however, a rule relating to immunity rather than admissibility,[16] since even improperly obtained privileged material may be admissible in evidence.[17]

10 Confidentiality in this context is properly understood in the broader sense of information that the lawyer is not at liberty to disclose and may include information about a client that is in fact in the public domain: see the decision of the House of Lords in *Hilton v. BBE* [2005] 1 WLR 567, para. 34.

11 *ISTIL Group Inc v. Zahoor* [2003] 2 All ER 252, para. 60 (*per* Lawrence Collins J).

12 See *Bourns Inc v. Raychem Corp* [1999] 3 All ER 154, 167, 168, CA.

13 *R v. Derby Magistrates Court, ex p B* [1996] AC 487, 507, 508, HL; *General Mediterranean Holdings SA v. Patel* [2000] 1 WLR 272; *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 7.

14 *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 7, HL (*per* Lord Hoffmann).

15 *R v. Derby Magistrates' Court, Ex p B* [1996] AC 487, 507 (*per* Lord Taylor CJ, with whom Lords Mustill and Lloyd agreed).

16 *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908, para. 5, HL (*per* Lord Phillips).

17 *Calcraft v. Guest* [1898] 1 QB 759, CA; *R v. Tompkins* (1977) 67 Cr App R 181. The party to whom the privilege belongs might, of course, apply for an injunction to restrain its use: *Ashburton v. Pape* [1913] 2 Ch 469, CA; *Goddard v. Nationwide Building Society* [1987] QB 670, CA.

The privilege is absolute and can only be overridden in very exceptional circumstances.[18] Furthermore, in accordance with the aphorism 'once privileged, always privileged',[19] once a client's privilege has attached to a document or other privileged exchange, the privilege will persist, subject only to waiver or other types of loss, for the client's benefit and that of successors in title for all time and in all circumstances.[20]

35.2.3 Rationale

The rationales underlying legal advice and litigation privilege are distinct:

- The interest protected by legal advice privilege is the public concern to ensure the availability of appropriate legal advice and assistance.[21] To this end, English law recognises the need to promote absolute candour between client and lawyer, by providing that exchanges between them will not subsequently be divulged.[22]
- Litigation privilege has often been regarded as an aspect of the right to a fair trial in England and in other common law jurisdictions.[23] The courts have emphasised that fairness requires a private and confidential sphere of preparation for litigation.[24] In a classic statement of this principle James LJ emphasised that 'as you have no right to see your adversary's brief, you have no right to see that which comes into existence merely as materials for that brief.'[25] Litigation privilege has therefore been characterised by Steyn LJ as an auxiliary principle buttressing the constitutional right of access to justice.[26] In recent judgments, this rationale has been doubted, largely on the grounds that changes to English civil procedure (particularly the rules of pretrial disclosure) have introduced a culture of openness, which sits uneasily with any right to

18 As Lord Scott stated in *Three Rivers No. 6* (para. 25): 'if a communication or document qualifies for legal professional privilege, the privilege is absolute. It cannot be overridden by some supposedly greater public interest. It can be waived by the person, the client, entitled to it, and it can be overridden by statute . . . but it is otherwise absolute. There is no balancing exercise that has to be carried out: see *B v. Auckland District Law Society* [2003] 2 AC 736, 756-759.'

19 For examples of its use see *Calcraft v. Guest* [1898] 1 QB 759, 761, CA; and *Pearce v. Foster* (1885) 15 QBD 114, 119, CA.

20 See *Thanki*, paras. 1.68 to 1.74. See also *Addlesee v. Dentons Europe LLP* [2019] EWCA Civ 1600.

21 See generally *Thanki*, paras. 1.17 to 1.22.

22 *Pearse v. Pearse* (1846) 1 De G & Sm 12, 28, 29 (*per* James Knight Bruce V-C), (cited with approval by Lord Carswell in *Three Rivers No. 6*, para. 112). See also *Pearce v. Foster* (1885) 15 QBD 114, 119 and 120 (*per* Sir Baliol Brett MR); *Re L* [1997] AC 16, 32 (*per* Lord Nicholls), (also cited with approval in *Three Rivers No. 6*, para. 112).

23 *Re Saxton* [1962] 1 WLR 968, 972 (*per* Lord Denning); *Baker v. Campbell* (1983) 49 ALR 385, 427 (*per* Brennan J).

24 *Three Rivers No. 6*, para. 52 (*per* Lord Rodger); *Robert Hitchins Ltd v. ICL* (CA, 10 December 1996), *per* Simon Brown LJ; *Sumitomo Corporation v. Credit Lyonnais Rouse Ltd* [2002] 1 WLR 479, para. 46, CA (*per* Jonathan Parker LJ).

25 *Anderson v. Bank of British Columbia* (1876) 2 Ch D 644, 656. See to similar effect *Waugh v. British Railways Board* [1980] AC 521, 531 (*per* Lord Wilberforce).

26 *Oxfordshire CC v. M* [1994] Fam 151, 163, CA.

'secrecy' in adversarial litigation.[27] However, litigation privilege remains justified by the need for a zone of privacy in the preparation for litigation[28] and remains firmly entrenched in English law as a consequence of decisions at appellate level, including the House of Lords.[29]

No adverse inference can be drawn where privilege is relied on 35.2.4

No adverse inferences may be drawn from the assertion by a person of a claim to legal professional privilege.[30] This is a principle that may sometimes be overlooked when an authority is seeking disclosure of privileged materials. But any responsible regulator or prosecuting authority must accept that it can neither require disclosure of privileged communications, nor rely on the regulated entity's refusal to provide it. As Lord Scott observed in *Three Rivers No. 6*, the existence of legal professional privilege means that 'cases may sometimes have to be decided in ignorance of relevant probative material.'[31]

There is, however, some uncertainty as to whether UK prosecuting authorities can require privilege to be waived when entering into co-operation agreements with parties.[32] In *R v. George*,[33] a case against certain British Airways executives concerned with a cartel offence involving alleged collusion with Virgin Atlantic, this issue arose in circumstances where the relevant Virgin Atlantic executives had admitted the offences and were given immunity from prosecution by the Office of Fair Trading (OFT).[34] Under the OFT's leniency and immunity guidelines, these executives were expected to assume an obligation of continuous and complete co-operation with the OFT's investigation and any subsequent proceedings. Owen J considered that it would be reasonable for the OFT to press for disclosure of privileged material in the hands of the Virgin Atlantic executives, as part of the OFT's duty to obtain material held by a third party that might be capable of undermining the prosecution case, on the basis that the Virgin Atlantic executives were under a duty to give continuous and complete co-operation as a condition of leniency or immunity and failing a satisfactory response to have invoked its power to revoke the leniency agreements.[35] By contrast, in *R v. Daniels*,[36] in which

27 See *Secretary of State for Trade & Industry v. Baker* [1998] Ch 356, 371 (*per* Sir Richard Scott V-C); *Visx Inc v. Nidex* [1999] FSR 91; *Three Rivers No. 6*, paras. 29 (*per* Lord Scott) and 53 (*per* Lord Rodger).

28 See *Thanki*, para. 3.153; *Passmore*, para. 3.022.

29 See *Thanki*, para. 1.25.

30 *Wentworth v. Lloyd* (1864) 10 HLC 589; *Sayers v. Clarke Walker* [2002] EWHC Ch 60, para. 52.

31 *Three Rivers No. 6* at para. 34.

32 See generally *Passmore*, paras. 1-077 to 1-085.

33 Unreported, 7 December 2009.

34 The OFT has now been superseded, along with the Competition Commission, by the Competition and Markets Authority (CMA), though regulation of consumer credit passed to the Financial Conduct Authority (FCA).

35 The case against the BA executives ultimately collapsed following the discovery of thousands of prosecution e-disclosure documents that had not been disclosed to BA or reviewed by the OFT.

36 [2010] EWCA Crim 2740.

a co-defendant to a murder charge had entered into an agreement pursuant to section 73 of the Serious Organised Crime and Police Act 2005 (SOCPA) under which he agreed to give assistance to the authorities, the Court of Appeal did not express a view as to whether a requirement to waive privilege could lawfully be included in a SOCPA agreement and indicated (without deciding) that, if so, an express condition would be required. The ability of a prosecuting authority to require waiver of privilege, and the circumstances in which it will be taken to have done so, therefore remains in some doubt and would appear to vary depending on the particular rules and guidelines applicable to the prosecuting authority. Since the decision in *R v. George*, the OFT guidance 'Applications for leniency and no-action in cartel cases' (the 2013 Leniency Guidance), now adopted by the CMA, has changed and no longer requires waiver of privilege as an element of co-operation. However, the CMA does not rule out enquiring as to whether a leniency applicant may be prepared to waive privilege over certain material during the course of a possible criminal cartel prosecution, although making it clear that any refusal to waive privilege will not have any adverse consequences for the leniency application and that granting such a waiver would not yield any advantage to the leniency applicant. The CMA will, unless the position is uncontroversial, instruct independent counsel to provide an opinion on whether the relevant information is privileged and will require disclosure of information not found to be privileged.[37] It is also clear that a party's willingness to waive privilege is a relevant factor to be taken into account by a court when considering, pursuant to section 45 and Schedule 17 of the Crime and Courts Act 2013, whether to approve a deferred prosecution agreement.[38]

35.2.5 Privilege belongs to the client

Privilege belongs to the client and not to the lawyer or agent.[39] Only the client can invoke the privilege.[40] It is not open to a lawyer or other agent to do so, unless acting on behalf of the client, and the lawyer or agent cannot invoke the privilege if the client has waived it.[41] In the case of litigation privilege, a third party

37 2013 Leniency Guidance paras. 3.15 to 3.23.

38 *Serious Fraud Office v. Rolls-Royce plc* [2017] Lloyd's Rep FC 249 at paras. 19 to 21, 35 to 39, 121; *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791 at para. 117.

39 *R v. Derby Magistrates' Court, ex p B* [1996] AC 487, 504, 505, HL.

40 Although the lawyer is under a professional obligation to assert the privilege on behalf of his or her client unless it has been waived: *R v. Central Criminal Court, ex p Francis and Francis* [1989] AC 346, 383, HL; *Bolkiah v. KPMG* [1999] 2 AC 222, 235, 236, HL; *Nationwide Building Society v. Various Solicitors* [1999] PNLR 52, 69. The court may also intervene to prevent a third party or even the client's lawyer making disclosure in breach of the client's privilege: *Harmony Shipping v. Saudi Europe Line* [1979] 1 WLR 1380, 1384, 1385, CA.

41 *Re International Power Industries* [1985] BCLC 128; *R v. Peterborough Justices, ex p Hicks* [1977] 1 WLR 1371; *Nationwide Building Society v. Various Solicitors (No. 2) The Times*, 1 May 1988.

with whom a lawyer or client has communicated for the purposes of adversarial proceedings may not assert the privilege of the party to the actual or prospective litigation.[42]

Legal advice privilege 35.3

The scope of legal advice privilege was the subject of authoritative reconsideration by the House of Lords in *Three Rivers No. 6*. Lord Rodger defined the privilege (at paragraph 50) as extending to:

> *[A]ll communications made in confidence between solicitors and their clients for the purpose of giving or obtaining legal advice even at a stage where litigation is not in contemplation. It does not matter whether the communication is directly between the client and his legal advisor or is made through an intermediate agent of either.*

The requirements thereby identified can be summarised as follows:

- a communication, whether written or oral;
- between a client and a lawyer (or an intermediate agent of either);
- made in confidence;[43]
- for the purpose of giving or obtaining legal advice.

Communication 35.3.1

The basic concept of communication is self-explanatory. However, privilege does not arise upon the exchange of pre-existing and previously unprivileged documents: the document's existence must be attributable to the intention to communicate.[44] The scope of the privilege is, however, broader than references merely to 'communications' might seem to indicate. In addition to communications, the following documents will also (if the remaining requirements are satisfied) fall within the privilege:

- a document intended to be a communication between client and lawyer, which was never communicated;[45]

42 *Lee v. SW Thames Health Authority* [1985] 1 WLR 845, CA; *Schneider v. Leigh* [1955] 2 QB 195.

43 This requirement has been considered in Section 35.2.1.

44 *Pearce v. Foster* (1885) 15 QBD 114, 118-119, CA; *R v. Peterborough Justices, ex p Hicks* [1977] 1 WLR 1371, 1374; *Ventouris v. Mountain* [1991] 1 WLR 607, 616, CA (*per* Bingham LJ).

45 *Three Rivers No. 6*, para. 21.

- documents or parts of documents that evidence the substance of lawyer–client communications.[46] This would include, for example, a written record of an oral communication or a document disseminating the contents or substance of legal advice within[47] or even beyond[48] the corporation receiving the advice; and
- the lawyer's working papers, including drafts, attendance notes and memoranda.[49]

35.3.2 Between a client and lawyer

35.3.2.1 Lawyer

The scope of the term 'lawyer' for the purposes of legal advice privilege (and legal professional privilege more generally) is broad rather than formalistic, but not without limits. In *R (Prudential PLC) v. Special Commissioner of Income Tax*, the Supreme Court confirmed that legal professional privilege is applicable only to 'communications in connection with advice given by members of the legal profession, which includes members of the Bar, the Law Society, and the Chartered Institute of Legal Executives (CILEX) (and, by extension, foreign lawyers)'.[50] The privilege extends to their non-qualified employees including secretaries,[51] clerks, trainee solicitors, pupils or paralegals acting under the direction of a lawyer.[52] For the avoidance of doubt, under English law[53] no distinction is made between in-house lawyers and lawyers in independent practice.[54] However, that an individual happens to be a 'lawyer' in the sense required above will not suffice; in each case the relevant question is whether he or she is consulted in that professional capacity.[55] The lawyer must also be subject to the control of the professional body and the governing rules of practice; in other words, the lawyer must have a current

46 *Three Rivers District Council and others v. Governor and Company of the Bank of England (No. 5)* [2003] QB 1556 (CA) (*Three Rivers No. 5*), paras. 19, 26.

47 *Bank of Nova Scotia v. Hellenic Mutual War Risks Association (Bermuda) Ltd (The Good Luck)* [1992] 2 Lloyd's Rep 540.

48 *USP Strategies Plc v. London General Holdings Ltd* [2004] EWHC (Ch) 373.

49 *Greenough v. Gaskell* (1833) 1 M&K 98, 101, 102 (entries made by the lawyer in his accounts held to be privileged); *Ainsworth v. Wilding* [1900] 2 Ch 315, 323 (*per* Stirling J) (notes or memoranda made by a lawyer are placed on the same footing as communications between lawyer and client); *Balabel v. Air India* [1988] Ch 317, 323 (*per* Taylor LJ); *Three Rivers No. 5*, para. 30.

50 *R (Prudential PLC) v. Special Commissioner of Income Tax* [2013] 2 AC 185, para. 29, SC. On communications with foreign lawyers, see *Thanki*, para. 1.52.

51 *Descoteaux v. Mierzwinski* (1982) 141 DLR (3d) 590, 603.

52 *Taylor v. Forster* (1825) 2 C&P 195; *Wheeler v. Le Marchant* (1881) 17 Ch D 675, 682, CA.

53 This is subject to one narrow exception: the European Court of Justice has held that, as a matter of European Community law, parties to investigations into alleged breaches of Articles 81 (now 101) and 82 (now 102) of the Treaty of Rome cannot claim legal professional privilege for internal communications with employees, even if the employee is acting as an in-house lawyer: *Akzo Nobel Chemicals Ltd v. European Commission*, Case C550/07 P.

54 *Alfred Crompton Amusement Machines Ltd v. Customs & Excise Comrs (No. 2)* [1972] 2 QB 102, 129, (*per* Lord Denning MR) CA. This conclusion was not challenged on appeal: *Alfred Crompton Amusement Machines Ltd v. Customs & Excise Comrs (No. 2)* [1974] AC 405, 430 and 431, HL.

55 *Minter v. Priest* [1930] AC 558, 581 (*per* Lord Atkin).

practising certificate. Therefore a qualified solicitor who has been struck off the roll is not a lawyer for the purposes of legal professional privilege,[56] unless the client in good faith does not know that the solicitor has been struck off.[57]

Subject to certain specific statutory exceptions,[58] communications with other professionals – including, for example, patent and trade mark attorneys – will not attract legal advice privilege at common law, even where they are giving advice on strictly legal matters.[59]

Legal advice privilege will apply to advice received from foreign lawyers.[60] It covers advice given by foreign lawyers on English law[61] as well as foreign law.[62]

Client 35.3.2.2

The concept of the 'client' in the context of corporations was the subject of appellate consideration by the Court of Appeal in *Three Rivers No. 5* and has recently been the subject of further consideration by the Court of Appeal in *The Director of the Serious Fraud Office v. ENRC* (which is discussed later in this section). The true *ratio* of *Three Rivers No. 5* has been the subject of controversy. In previous editions of this work, it was said that it appeared that the 'client' would not necessarily be the corporation itself, or its employees *per se*, but only those within the corporation who were authorised to communicate with the lawyer and receive his or her advice.[63] This was the interpretation of *Three Rivers No. 5* adopted by the Singapore Court of Appeal in *Skandinaviska Enskilda Banken v. Asia Pacific Breweries*. The court in that case commented that: 'The principle is that if an employee is not authorised to communicate with the company's solicitors for the

56 *Dadourian Group International and others v. Simms and others* [2008] EWHC 1784 (Ch), paras. 119 to 28. See also *Waterford v. Commonwealth of Australia* (1987) 163 CLR 54, 81, 82 (*per* Deane J).

57 *Dadourian Group International and others v. Simms and others* [2008] EWHC 1784 (Ch), para. 127. The burden is on the client to show that he or she continued to believe that the solicitor held a practising certificate at the time.

58 For example: patent attorneys (section 280, Copyright, Designs and Patents Act 1988); trade mark attorneys (section 284, Copyright, Designs and Patents Act 1988); licensed conveyancers (section 33, Administration of Justice Act 1985); authorised advocates and litigators (section 63, Courts and Legal Services Act 1990). It is clear that patent and trade mark attorneys do not attract legal professional privilege at common law: *Dormeuil Trade Mark* [1983] RPC 131; *Wilden Pump Engineering Co v. Fusfield* [1985] FSR 159, CA; *R (Prudential plc) v. Special Commissioner of Income Tax and Pandolfo* [2013] 2 AC 185, para. 68.

59 *R (Prudential Plc) v. Special Commissioner of Income Tax and Pandolfo* [2013] 2 AC 185. See R Pattenden, The Law of Professional–Client Confidentiality (2003), para. 16.42, for a comprehensive list of other professions to which privilege has been expressly denied, including doctors, accountants, priests, bankers, auditors and journalists.

60 See, most recently, *R (Prudential PLC) v. Special Commissioner of Income Tax and Pandolfo* [2013] 2 AC 185, paras. 45, 73.

61 *International Business Machines Corp v. Phoenix International (Computers) Ltd* [1995] 1 All ER 413, 429; *Ritz Hotel Ltd v. Charles of the Ritz Ltd (No. 4)* (1987) 14 NSWLR 100 to 102.

62 *Bunbury v. Bunbury* (1839) 2 Beav 173; *Macfarlan v. Rolt* (1872) LR 14 Eq 580.

63 See *Three Rivers No. 5*, para. 31 (*per* Longmore LJ, giving the judgment of the Court of Appeal).

purpose of obtaining legal advice, then that communication is not protected by legal advice privilege.' It went on to state that authorisation need not be express but may be implied.[64]

However, the concept of the 'client' was interpreted more restrictively in two first-instance decisions of the English High Court.[65] In *The RBS Rights Issue Litigation*[66] Hildyard J held that notes of witness interviews prepared by RBS's lawyers were not subject to legal advice privilege (although the interviewees were authorised by RBS to communicate with the lawyers), and neither were the notes subject to legal advice privilege on the basis that they comprised lawyers' working papers. In Hildyard J's view, the Court of Appeal in *Three Rivers No. 5* established a general principle that 'the client' for the purposes of a lawyer–client communication subject to legal advice privilege must be someone who is authorised to seek and receive legal advice. The approach in *The RBS Rights Issue Litigation* was followed by Andrews J in the first-instance decision in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation*,[67] where once again the privileged status of interview notes produced by the lawyers during the course of an internal investigation was in issue. Andrews J held that legal advice privilege attaches only to 'communications between the lawyer and those individuals who are authorised to obtain legal advice on that entity's behalf.'[68] By 'authorised' Andrews J meant being specifically 'tasked' by the corporation to obtain legal advice, a qualification not found in the judgment of the Singapore Court of Appeal in the *Skandinaviska* case referred to above. That interviewees were authorised to communicate with the lawyers to provide them with information or relevant facts in order for the lawyers to give advice, did not make those communications privileged. Andrews J also agreed with Hildyard J that lawyers' notes of interviews with witnesses would not be privileged on the ground of being lawyers' working papers, unless the notes would betray the tenor of the legal advice.

64 *Skandinaviska Enskilda Banken AB (Publ), Singapore Branch v. Asia Pacific Breweries (Singapore) Pte Ltd* [2007] 2 SLR 367, para. 42.

65 A similar approach was also taken by Chief Master March in *Astex v. Astrazeneca* [2016] EWHC 2759 (Ch) and by the Divisional Court in *R(AL) v. Serious Fraud Office* [2018] EWHC 856 (Admin) (although the reasoning on this issue in that case is somewhat confused, perhaps because – on the unusual facts of the case – no party was positively asserting that privilege applied to the interview notes in question).

66 *The RBS Rights Issue Litigation* [2016] EWHC 3161 (Ch).

67 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2017] 1 WLR 4205.

68 Ibid., at para. 70. Andrews J acknowledged that, in the context of a company, the person giving the instructions to the lawyers may not necessarily be the same as the person or persons who want to receive the advice. Accordingly, there could be instances where particular individuals or groups are authorised to instruct the lawyers, while others individuals are authorised to receive the advice, typically a company's board of directors (see ibid., at para. 84).

The issue came before the Court of Appeal in *The Director of the Serious Fraud Office SFO v. ENRC.*[69] The Court analysed the decision in *Three Rivers No. 5* and concluded as follows:

> *We can fully accept that the Court of Appeal could have decided* Three Rivers (No. 5) *on the simple basis that Freshfields' client was the BIU (not the Bank), and the documents had been prepared by the Bank (not the BIU), so that the position of the particular Bank employee who had prepared them was irrelevant to the question of legal advice privilege. We do not, however, think that, fairly read, that was the Court of Appeal's reasoning. . . . it seems to us that Longmore LJ reasoned that, because agents and employees, on authority, stood in the same position in relation to legal professional privilege, once it was established that only communications between the lawyer and the client, and not between the lawyer and an agent of the client, could attract legal advice privilege, communications between a lawyer and an employee of the client (other than employees specifically tasked with seeking and receiving legal advice) could also not be privileged. As we have said, we are not sure that it is necessary for us to determine whether this reasoning was the* ratio decidendi*, but if that did have to be decided, we would hold that it was.*[70]

As to whether *Three Rivers No. 5* was correctly decided on this point, the Court of Appeal in *ENRC* held[71] that this is a question which can only be determined by the Supreme Court. Nevertheless, the Court expressed the view that there was 'much force' in submissions made on behalf of ENRC and The Law Society (intervening in the appeal) that, if *Three Rivers No. 5* did indeed decide that the definition of 'client' should be restrictively interpreted as it was in *The RBS Rights Issue Litigation*, then it was wrongly decided. The Court referred to the policy justification for legal advice privilege, that there is a public interest in a client being able to place all the facts before the legal adviser without fear that they may afterwards be disclosed and used to the client's prejudice, and to the fact that large corporations need, as much as small corporations and individuals, to seek and obtain legal advice without fear of intrusion. The Court acknowledged that, in the modern world, legal advice is often sought by large national and multinational companies where the information on which legal advice is sought is unlikely to be in the hands of the main board or those it appoints to seek and receive legal advice; therefore:

> *If a multi-national corporation cannot ask its lawyers to obtain the information it needs to advise that corporation from the corporation's employees with relevant first-hand knowledge under the protection of legal advice privilege,*

69 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791.

70 Ibid., at para. 81.

71 Ibid., at para. 124.

> *that corporation will be in a less advantageous position than a smaller entity seeking such advice. In our view, at least, whatever the rule is, it should be equally applicable to all clients, whatever their size or reach.*[72]

The Court also referred to English law being, on this issue, out of step with the international common law and remarked on the undesirability of such inconsistency. The Court concluded that:

> *If, therefore, it had been open to us to depart from* Three Rivers (No. 5)*, we would have been in favour of doing so. For the reasons we have given, however, we do not think that it is open to us, so it is a matter that will have to be considered again by the Supreme Court in this or an appropriate future case.*[73]

The Court of Appeal in *ENRC* upheld ENRC's claim to privilege over the relevant interview notes on grounds of litigation privilege, overturning the judgment of Andrews J at first instance, and it was therefore strictly unnecessary for it to consider the issue of who may constitute 'the client', which only arose in the context of the alternative claim to legal advice privilege. It might therefore be argued that the Court's reasoning on this point is technically *obiter*. However, it is at the very least highly persuasive guidance as to why, in a corporate context, a restrictive approach as to who may constitute 'the client' for the purposes of legal advice privilege is undesirable and unworkable as a matter of policy and principle. If the issue finally reaches the Supreme Court,[74] there is every chance that the restrictive interpretation of 'client' will be reconsidered but, until then, the law should be taken to be as stated by the Court of Appeal in *ENRC*.

The implications of a restrictive interpretation of 'client' in a corporate context are well rehearsed. This approach is likely to exclude the vast majority of employees within the company. A corporate entity that wishes to obtain legal advice and that needs to carry out a fact-finding investigation within the organisation to obtain the necessary information for its lawyers will not, while these decisions on the proper interpretation and application of *Three Rivers No. 5* remain good law, be able to claim legal advice privilege over documents created pursuant to that fact-finding investigation (except, it seems, to the extent that the facts are known to, and obtained by the lawyers from, individuals who also happen to be authorised to seek and receive legal advice). While the rationale of legal advice privilege is, as explained in Section 35.2.3, to enable a client to provide full and frank instructions to its lawyer to enable the lawyer to provide sensible advice, it appears that (pending any clarification from the Supreme Court) a corporate client will be severely restricted in the extent to which it can gather information for its lawyer in order for the lawyer to give advice without its communications being

72 Ibid., at para. 127.

73 Ibid., at para. 130.

74 The issue will need to be clarified in another case as the Serious Fraud Office (SFO) did not pursue an application for permission to appeal to the Supreme Court in *ENRC*.

disclosable in subsequent proceedings. It makes no difference whether information is obtained from employees by other employees of the company or by the lawyers directly.

In this regard, and as recognised by the Court of Appeal in *ENRC*, English law is also at odds with other common law jurisdictions. The Hong Kong Court of Appeal in *CITIC Pacific v. Secretary of State for Justice*[75] recognised that a narrow definition of client was incompatible with the rationale for legal advice privilege as explained by the House of Lords in *Three Rivers No. 6*. The decisions in *The RBS Rights Issue Litigation* and, at first instance, in *ENRC* also seem to be doubtful in relation to the lawyers' working papers doctrine. Notes of witness interviews that are prepared by lawyers, provided they are not verbatim transcripts, are types of document that should typically qualify as 'lawyers working papers', in line with the decision in *Balabel v. Air India*.[76] This was the subject of argument before the Court of Appeal in *ENRC*. However, the Court declined to decide this issue because, in light of its findings on litigation privilege, it did not strictly arise and moreover the Court considered that it would be preferable for the matter to be addressed by the Supreme Court in the context of any future consideration of legal advice privilege.[77]

Communication need not in all cases be direct, but may occur through an agent of the client or the lawyer. A distinction needs to be made between an agent for the purposes of communication, that is to say a mere conduit between the client and the lawyer, such as an interpreter (where intellectual input by the agent will risk destroying the privilege[78]) and an agent for the purposes of seeking and obtaining the advice (where it will not). Communications between 'the various legal advisers of the client' with a view to the client obtaining legal advice or assistance will generally be privileged.[79]

75 [2012] 2 HKLRD 701.

76 In this regard there must be some doubt as to whether the court was correct in *The RBS Rights Issue Litigation* and in *ENRC* – at first instance – in stating that to qualify as lawyers' working papers, documents must betray the trend of legal advice. That is not a requirement specified in *Balabel* (in which the Court of Appeal was considering a claim to privilege in respect of both communications between client and lawyer and lawyers' working papers) nor is it required in *Three Rivers No. 5* itself. In specifying that requirement Hildyard J in *The RBS Rights Issue Litigation* and Andrews J in *ENRC* relied on observations made in a different context, namely where a solicitor copies or assembles a collection of documents, and the issue is whether that selection can be said to be privileged (see *Lyell v. Kennedy (No. 3)* (1884) 27 Ch D 1; subsequently commented on by Bingham LJ in *Ventouris v. Mountain* [1991] 1 WLR 607.)

77 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, paras. 141, 142.

78 See *Thanki*, para. 2.77.

79 *Trade Practices Commission v. Sterling* (1979) 36 FLR 244, para. 4.

35.3.3 For the purpose of giving or obtaining legal advice or assistance

In *Three Rivers No. 6*, the House of Lords unanimously[80] adopted a statement by Taylor LJ in *Balabel v. Air India*[81] that:

> *[L]egal advice is not confined to telling the client the law; it must include advice as to what should prudently and sensibly be done in the relevant legal context.*

In most cases the relevant 'legal context' will be obvious. Where there is room for doubt, Lord Scott suggested[82] that the court should consider whether:

- the advice sought from the lawyer relates to the rights, liabilities, obligations or remedies of the client either under private or public law; and
- the communication falls within the policy underlying the justification for legal advice privilege. In short, 'is the occasion on which the communication takes place and is the purpose for which it takes place such as to make it reasonable to expect the privilege to apply?'

Notwithstanding the first limb of Lord Scott's test, it appears that the 'legal context' is not actually confined to advice concerning the client's legal rights and liabilities. The relevant communications in *Three Rivers No. 6* involved presentational advice as to how the client (the Bank of England) could best put material before an inquiry, established by the Chancellor of the Exchequer and the Governor of the Bank, which was scrutinising the discharge of the Bank's public duties. The House of Lords held that legal advice privilege plainly applied. Lord Rodger emphasised[83] that privilege would similarly have applied 'to presentational advice sought from lawyers by any individual or company who believed himself, herself or itself to be at risk of criticism by an inquiry', emphasising that the 'defence of personal reputation and integrity is at least as important to many individuals and companies as the pursuit or defence of legal rights whether under private law or public law'.

In substance, the test is whether the lawyer is reasonably being consulted because of his or her legal skills. This is reflected in the emphasis placed by the House of Lords on whether the lawyer is being consulted '*qua* lawyer',[84] or is being asked to 'put on legal spectacles'[85] and whether the lawyer is being required to exercise 'special professional knowledge and skills'.[86] The concept of a 'legal context' is therefore very broad.

80 *Three Rivers No. 6*, paras. 38, 59, 62, 111, 122.
81 [1988] Ch. 317, 330, CA.
82 *Three Rivers No. 6*, para. 38.
84 Ibid., at para. 58 (*per* Lord Rodger).
85 Ibid., at para. 60 (*per* Lord Rodger).
86 Ibid., at para. 62 (*per* Baroness Hale).

Once a 'legal context' is established, the question is whether the relevant communication falls within it. The clearest definition of the ambit of legal advice in *Three Rivers No. 6* was that provided by Lord Carswell (with whom all the Law Lords expressly agreed[87]), in the following passage:

> *[A]ll communications between a solicitor and his client relating to a transaction in which the solicitor has been instructed for the purpose of obtaining legal advice will be privileged, notwithstanding that they do not contain advice on matters of law or construction, provided that they are directly related to the performance by the solicitor of his professional duty as legal adviser of his client.*[88]

This passage can be regarded as an authoritative statement of the modern law. If the larger purpose of the instruction is the obtaining of legal advice, the question in respect of any given communication is simply whether it relates directly to the lawyer's performance of his duty as the client's legal adviser. The House of Lords expressly rejected any requirement that the communication must itself contain 'legal advice', in any strict sense of that phrase. *Three Rivers No. 6* therefore both preserves and consolidates a line of authority that supports the attachment of privilege to documents that, while they do not contain legal advice, nevertheless form part of the 'continuum of communications' made for that broad purpose.

The law as stated above was given effect in the regulatory investigations context in the case of *Property Alliance Group v. RBS*.[89] In that case RBS claimed privilege over documents prepared by its solicitors for the RBS Executive Steering Group (ESG), which had been established by RBS to oversee its response to various regulatory and criminal investigations into manipulation of LIBOR and other rates in the United Kingdom, United States and elsewhere. The claimant, Property Alliance Group (PAG), challenged RBS's claim to privilege over these documents, contending that the role of RBS's solicitors was not confined to the provision of legal advice but extended to the performance of administrative functions (for example, acting as the secretariat for the ESG and attending its meetings) for which privilege could not be claimed. Having inspected the disputed documents, Snowden J was 'entirely satisfied' that RBS's solicitors had been engaged in a relevant legal context. He remarked that:

> *RBS was facing Regulatory Investigations in a number of jurisdictions that could have had (and did have) the consequence that RBS was subjected to very large regulatory penalties and consequent private actions for very significant sums of money. Dealing with, and co-ordinating the communications and responses to such regulators was a serious and complex matter upon which RBS*

87 Ibid., at paras. 45, 49, 61, 119.

88 Ibid., at para. 111 (emphasis added).

89 [2016] 1 WLR 992. See also *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2017] 1 WLR 4205, at para. 184.

> *naturally wished to have the advice and assistance of specialist lawyers. Clifford Chance were engaged to provide such advice and assistance, and (to use Lord Scott's words), that advice and assistance undoubtedly related to the rights, liabilities and obligations of RBS, and the remedies that might be granted against it either under private law or under public law.*
>
> *I am also entirely satisfied that, in the words of Taylor LJ in [*Balabel*] the two types of ESG High Level Documents* [i.e. tabular memoranda informing and updating the ESG on the progress, status and issues arising in the regulatory investigations, and confidential notes or summaries drafted by Clifford Chance concerning the discussions between the ESG and its legal advisers at the ESG meetings] *form part of 'a continuum of communication and meetings' between Clifford Chance and RBS, the object of which was the giving of legal advice as and when appropriate.*[90]

Snowden J also rejected an argument made by PAG that the ESG documents should be only partly redacted, so that summaries of factual information would not be withheld from inspection, finding that such an approach would be inconsistent with the *dicta* of Taylor LJ in *Balabel*.[91] While, depending on the facts, a court might not uphold a claim to privilege in respect of the minutes of a business meeting simply because the minutes were taken by a lawyer who was present and subsequently sent them to the client, that would be because the court would have taken the view that the lawyer was not being asked *qua* lawyer to provide legal advice.

As to the public policy implications of his judgment, Snowden J noted (at paragraph 45) that there is a clear public interest in regulatory investigations being conducted efficiently and in accordance with law and that the public interest will be advanced if regulators can deal with experienced lawyers who can accurately advise their clients how to respond and co-operate. Such lawyers must be able to give the client candid factual briefings as well as legal advice, secure in the knowledge that any such communications and any record of their discussions and the decisions taken will not subsequently be disclosed without the client's consent.

35.3.4 Communications with multiple addressees

A difficult question that frequently arises in practice, particularly where in-house lawyers are involved, is how to determine the privileged status of communications (typically emails) to which a number of people are party, only one of whom is a lawyer. This issue was addressed in the recent case of *R (on the application of Jet2.com) v Civil Aviation Authority*.[92] In this judicial review claim Jet2.com is challenging the decision of the Civil Aviation Authority (CAA) to publish a press release about Jet2.com's refusal to participate in a new alternative dispute resolution scheme proposed for the aviation industry and the CAA's decision to publish

90 *Property Alliance Group v. RBS* [2016] 1 WLR 992, at paras. 27, 28.

91 *Balabel v. Air India* [1988] Ch 317 at 330F.

92 [2018] EWHC 3364 (Admin).

correspondence between it and Jet2.com about that press release. In Jet2.com's application for disclosure of, *inter alia*, internal documents at the CAA relating to the drafting of the letter it had written to Jet2.com in response to its complaint, issues arose as to the application of legal advice privilege as a result of the involvement of in-house lawyers in the discussion and drafting of the letter.

The Administrative Court made two findings in relation to privilege issues. First, it held that legal advice privilege is subject to a dominant purpose test (i.e., the communication will only be privileged if it was bought into existence with the dominant purpose of it or its contents being used to obtain legal advice). This is very controversial, and in the authors' view incorrect in law.[93]

The second finding was in relation to the assessment of the privileged status of multi-addressee communications (a communication sent to multiple recipients including a lawyer). The Court said that the correct approach was a two-stage one. First, it is necessary to determine whether the dominant purpose of the email (or an attachment to that email) is to seek or give legal advice; if it is, then the communication will be privileged. If the dominant purpose test is not, however, met, it is then necessary to turn to the second stage and assess whether the email (or its attachment) discloses, or is likely to disclose, or may disclose, the nature and content of the legal advice sought from or given by the lawyer. If it does, then the email (or attachment, as the case may be) is privileged. If not, the communication is not privileged. The clear implication of the judgment is that emails and their attachments are to be treated as separate communications for the purposes of assessing their privilege status.

This decision is potentially problematic. While there is no clear authority as to how multi-addressee communications are to be approached for the purposes of assessing privilege, the Court's approach would appear to be contrary to the established principles as to the scope and application of legal advice privilege set out in *Three Rivers (No. 6)*. As noted above, the touchstone for legal advice privilege is whether the communication was made confidentially for the purposes of legal advice. Where information is passed by the solicitor or client to the other as part of the continuum aimed at keeping the other informed so that advice may be sought and given as required, privilege will attach. However, the effect of this judgment is that there will potentially be communications between legal advisers and the client, also sent or copied simultaneously to other individuals which, although part of the continuum of communication between lawyer and client, and despite having a relevant legal context, will not be privileged. In other words, the copying in of another individual or individuals into the email between lawyer and client may have the effect that privilege is lost. Moreover, the approach that an email and its attachment are to be treated as two communications or documents rather than one is also controversial.[94] The *Jet2.com* decision is the subject

93 For example, the Court of Appeal in *ENRC* noted (albeit *obiter*) that there was no such test in English law. See [2019] 1 WLR 791, para. 132.

94 A similar issue arose in *The Financial Reporting Council v. Sports Direct International plc* [2019] 2 All ER 974, in which the High Court rejected Sports Direct International's argument that legal

of an appeal, which is due to be heard in December 2019. It therefore remains to be seen whether these approaches to determining whether legal advice privilege applies will be upheld.

35.4 Litigation privilege

The leading modern statement of the scope of litigation privilege is contained in the speech of Lord Edmund-Davies in *Waugh v. British Railways Board*:

> *After considerable deliberation, I have finally come down in favour of the test propounded by Barwick C.J. in* Grant v. Downs*, 135 C.L.R. 674, in the following words, at p 677:*
>
> > *'Having considered the decisions, the writings and the various aspects of the public interest which claim attention, I have come to the conclusion that the court should state the relevant principle as follows: a document which was produced or brought into existence either with the dominant purpose of its author, or of the person or authority under whose direction, whether particular or general, it was produced or brought into existence, of using it or its contents in order to obtain legal advice or to conduct or aid in the conduct of litigation, at the time of its production in reasonable prospect, should be privileged and excluded from inspection.'*
>
> *Dominant purpose, then, in my judgment, should now be declared by this House to be the touchstone.*[95]

Litigation privilege can therefore be described as the privilege of a client to withhold from disclosure:

- oral or written communications between the client or the lawyer (on the one hand) and third parties (on the other) or other documents created by or on behalf of the client or the lawyer;
- that come into existence once litigation is in contemplation or has commenced; and
- that come into existence for the dominant purpose of obtaining information or advice in connection with, or of conducting or aiding in the conduct of, such litigation.

35.4.1 Communications or other documents

Litigation privilege will apply to communications between the client or the lawyer and third parties for the relevant purpose. In the case of client–third party communications there is no requirement that the lawyer either requests the client to

advice privilege can be claimed in respect of a document that is not privileged in itself, because it is attached to an email sent by a client to a lawyer seeking advice or by a lawyer to a client giving advice. As noted below, that decision is also under appeal.

95 [1980] AC 521, 543, 544 (emphasis added).

contact the third party[96] or that the communications are actually referred on to the lawyer.[97] In fact, no lawyer need have been engaged at the time of the communication.[98] In light of the narrow definition of 'client' in *Three Rivers No. 5*, as restrictively applied in subsequent decisions, many 'internal' communications within a corporation risk being characterised as communications between the client and 'third parties'. For example, where, as in *Three Rivers No. 5* itself, the corporation sets up a specific committee to deal with the relevant litigation, communications between a member of that committee and a non-committee employee of the corporation are likely to be characterised as communications between client and third party subject to whether the employee is authorised to give instructions or receive advice on behalf of the corporation.

See Section 35.3.2.2

The privilege will also cover material, aside from communications, brought into existence in furtherance of the litigation purpose. The cases have traditionally spoken in terms of granting protection to the 'materials for the brief'.[99] A modern restatement of this principle is that, in an adversarial system 'each party should be free to prepare his case as fully as possible without the risk that his opponent will be able to recover the material generated by his preparations.'[100] As regards documents actually brought into existence by a client's lawyer, the better view is that these are in fact protected by legal advice privilege.[101] The 'materials for the brief' concept would apply to preparatory documents generated by the client that do not embody communications with third parties (such as a client's working notes or internal oral or documentary communications). Provided the document satisfies the other requirement of litigation privilege (as to which see below), it will also apply to a document generated for the purpose of being shown to a prospective adversary in circumstances where the document has not, or not yet, been shared with that adversary.[102]

See Section 35.3

96 *Southwark and Vauxhall Water Company v. Quick* (1878) 3 QBD 315, 320 (per Brett LJ), 322 (*per* Cotton LJ).

97 Ibid., at 320 (*per* Brett LJ), 323 (*per* Cotton LJ).

98 *Re Highgrade Traders Ltd* [1984] BCLC 151, 172 (*per* Oliver LJ); *Buttes Gas and Oil Co v. Hammer (No. 3)* [1981] QB 223, 243 (*per* Lord Denning MR).

99 *Southwark and Vauxhall Water Company v. Quick* (1878) 3 QBD 315, 320 (*per* Brett LJ); *Lyell v. Kennedy (No. 2)* (1883) 23 Ch D 387, 404 (*per* Cotton LJ).

100 *Three Rivers No. 6*, para. 52 (*per* Lord Rodger).

101 See also *Thanki*, paras. 2.56 to 2.60, 3.27.

102 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, at para. 102.

35.4.2 Litigation commenced or in contemplation

See Section 35.2.3

In view of the underlying rationale of litigation privilege, the 'litigation' in question must be adversarial in nature.[103] Furthermore, the litigation must be 'reasonably in prospect'.[104] This matter was considered by the Court of Appeal in *USA v. Philip Morris Inc*.[105] In summary, it is not sufficient if there is simply a general apprehension of future litigation.[106] The requirement that litigation be 'reasonably in prospect' is not satisfied unless parties seeking to claim privilege can show that they were aware of circumstances that rendered litigation between themselves and a particular person or class of persons a real likelihood rather than a mere possibility; identifying potential causes of action and defendants to possible claims falls short of the necessary threshold.[107] By the same token, however, litigation need not be likely, in the sense of there being more than a 50 per cent chance of it occurring.[108]

The English courts apply a common-sense approach. Hence, litigation may be considered reasonably in prospect even if the cause of action has not yet arisen[109] or the party has not yet decided whether to take legal advice.[110] If litigation was reasonably in prospect when the communication or document was made, it does not matter if that litigation never commences.[111] Moreover, the litigation in which the privilege is later relied on need not concern the same subject matter or the same parties as the litigation in respect of which the privilege originally arose.[112]

The issue of when litigation may be said to be reasonably in contemplation was the subject of extensive consideration in *ENRC*. In that case, the defendant, ENRC, claimed litigation privilege in respect of documents created during the course of an investigation conducted by its lawyers that was initially prompted by a whistleblower report. The documents were created against the background of an anticipated criminal investigation by the Serious Fraud Office (SFO) and during a period of engagement between the SFO and ENRC (which the SFO contended was part of a self-reporting process).

---

103 See *In re L (a Minor) (Police Investigation: Privilege)* [1997] AC 16 (HL) (litigation privilege was held to be inapplicable to the particular wardship proceedings in question, which were inquisitorial rather than adversarial in nature). The Upper Tribunal noted in *LM v. London Borough of Lewisham* [2009] UKUT 204 that *Re L* did not decide that there is never any litigation privilege in care proceedings but that their Lordships had confined themselves to cases where the filing of a report requires the leave of the court in order that documents already filed in the proceedings may be disclosed to the expert or that the child nay be examined.

104 *Hellenic Mutual War Risks Association (Bermuda) Ltd v. Harrison (The Sagheera)* [1997] 1 Lloyd's Rep 160, 166 (*per* Rix J); *USA v. Philip Morris Inc* [2004] EWCA Civ 330, CA, para. 68; *Three Rivers No. 6*, para. 83 (*per* Lord Carswell).

105 [2004] EWCA Civ 330.

106 Ibid., at para. 68.

107 *Rawlinson & Hunter Trustees SA v. Akers* [2014] EWCA Civ 136, para. 24.

108 Ibid., at para. 65.

109 *Mayor and Corporation of Bristol v. Cox* (1884) 26 Ch D 678 (*per* Pearson J).

110 *Guinness Peat Properties v. Fitzroy Robinson Partnership* [1987] 1 WLR 1027, 1035, 1036 (*per* Slade LJ).

111 See *The Aegis Blaze* [1986] 1 Lloyd's Rep 203, 204 (*per* Parker LJ).

112 Ibid., at 210.

The judge at first instance, Andrews J, accepted that ENRC contemplated that it would be subject to a raid by the SFO, and that it reasonably contemplated a criminal *investigation* by the SFO, but found that this did not amount to anticipation of adversarial *litigation*.

She also rejected the submission that once ENRC contemplated a criminal investigation by the SFO, criminal prosecution was also in reasonable contemplation. In particular, she in effect drew a distinction between criminal and civil proceedings, finding that, for the purpose of a claim to litigation privilege where criminal proceedings are said to have been contemplated, the relevant party must have uncovered some evidence of wrongdoing before proceedings could be said to be in reasonable contemplation – otherwise there would be insufficient grounds for believing that a prosecution was likely.[113] She held that unless the relevant party had uncovered evidence of wrongdoing it could not consider the evidential test for the bringing of a criminal prosecution was likely to be met.[114] The implication of that approach seemed to be that for a party to establish that litigation was a real likelihood, it was required to adduce evidence that was itself likely to betray the privilege being asserted and would tend to be self-incriminating (because it would need to identify matters discovered during the investigation leading it to believe that prosecution was likely and not merely possible). This approach (which had been the subject of much criticism following the first-instance decision in *ENRC*) was firmly rejected by the Court of Appeal, which found that the contemporaneous documents demonstrated that ENRC was aware of circumstances that rendered litigation between itself and the SFO a real likelihood rather than a mere possibility (so satisfying the test in *Philip Morris*), although uncertainty remained as to what the internal investigation would uncover. In particular, ENRC was in receipt of a whistleblower report making serious allegations of corruption and financial wrongdoing that it had appointed lawyers to investigate, and internal emails showed that senior figures within ENRC were anticipating an SFO raid and investigation. There had also been correspondence from the SFO where the subtext, so the Court found, was the possibility, if not the likelihood, of prosecution if the self-reporting did not result in a civil settlement. The Court indicated that, while not every manifestation of concern by the SFO is likely to be regarded as adversarial:

> *[W]hen the SFO specifically makes clear to the company the prospect of its criminal prosecution (over and above the general principles set out in the [Self-Reporting] Guidelines), and legal advisers are engaged to deal with that situation, as in the present case, there is a clear ground for contending that criminal prosecution is in reasonable contemplation.*[115]

113 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2017] 1 WLR 4205 (Ch), at para. 160.

114 Ibid., at para. 151.

115 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, para. 96.

Further, while it cannot be assumed that, once an SFO criminal investigation is reasonably in contemplation, so too is a criminal prosecution, on the facts of *ENRC* the evidence pointed clearly towards the contemplation by ENRC of a prosecution if the self-reporting process did not avert it. The Court of Appeal rejected the idea that because further investigations were required before a party could say with certainty that proceedings were likely that this would prevent proceedings from being in reasonable contemplation, and it rejected the judge's distinction between civil and criminal proceedings. Corporate parties who face the threat of SFO investigation and prosecution may take some comfort from the Court of Appeal's guidance that: 'It would be wrong for it to be thought that, in a criminal context, a potential defendant is likely to be denied the benefit of litigation privilege when he asks his solicitor to investigate the circumstances of any alleged offence.'[116]

The Court of Appeal in *ENRC* also distanced itself from the decision of the Court of Appeal Criminal Division in *R (for and on behalf of the Health and Safety Executive) v Paul Jukes*.[117] In that case, the defendant had signed a statement shortly after a fatal industrial accident accepting that he was responsible for the company's health and safety. The Court in that case upheld the judge's decision that the statement was not covered by litigation privilege because criminal proceedings were not in contemplation and any privilege would anyway have attached to the company, which had not asserted it. The Court in *Jukes* had approved of Andrews J's distinction (at first instance in *ENRC*) between criminal and civil proceedings when considering whether proceedings were reasonably in contemplation. However, the Court of Appeal in *ENRC* held that *Jukes* was a decision on the facts and that the approval of Andrews J's approach was *obiter*. The effect of the decision of the Court of Appeal in *ENRC* is such that *Jukes* is likely to be marginalised and its apparent endorsement of Andrews J's approach to anticipation of litigation in a criminal context disregarded.

While the Court of Appeal's decision in *ENRC* has brought useful clarity as to the circumstances in which the first limb of the litigation privilege test may be satisfied, particularly in a corporate criminal context, there still remains some uncertainty as to exactly when regulatory proceedings may be regarded as sufficiently adversarial to meet the first limb. (The adversarial nature of the contemplated proceedings in *ENRC* was not in doubt, and the question of what type of regulatory action may engage litigation privilege was not directly addressed in *ENRC*). Some guidance can be found in *Tesco v. OFT*,[118] where the Competition Appeal Tribunal (CAT) was required to consider whether certain enforcement proceedings brought by the Office of Fair Trading were 'litigation' for the purpose of claiming litigation privilege. The decision concerned the OFT's investigation into dairy retail price-sharing between various supermarkets and dairy processors. In September 2007, the OFT issued a statement of objections against a number

116 Ibid., at para. 99.

117 [2018] Lloyd's Rep FC 157.

118 [2012] CAT 6.

of undertakings, including Tesco, alleging violation of the prohibition on anti-competitive agreements and practices. The OFT issued a supplemental statement of objections, in support of its case, in July 2009 and made its infringement decision in July 2011. On Tesco's appeal to the CAT, the OFT sought disclosure from Tesco of records of interviews with employees of other companies allegedly involved in Tesco's infringing conduct in the first half of 2011. Tesco resisted the application on the ground (among others) that the records were covered by litigation privilege.

The CAT refused the OFT's application for disclosure on the primary ground that such disclosure was not necessary, relevant and proportionate. However, it also considered the application of litigation privilege, finding that at the stage when Tesco contacted the potential witnesses the ongoing proceedings could properly be characterised as 'adversarial'. It was relevant that the statement, and supplementary statement, of objections had been issued and Tesco was contesting the allegations, that the OFT was determining Tesco's liability for a potential breach of the Competition Act and Tesco faced the possibility of a significant fine as a result, and that the proceedings were regarded as criminal for the purposes of Article 6 of the European Convention on Human Rights. The Chairman of the Tribunal also had regard[119] to the underlying rationale of fairness that underpins litigation privilege, finding that a fair procedure included the right of Tesco to present its case and to gather evidence, and that, as a corollary, litigation privilege applied to the relevant contacts with third-party witnesses.

The decision of the CAT confirmed that entitlement to claim litigation privilege in the context of regulatory enforcement proceedings will depend on the specific circumstances of the regulatory procedure and the stage it has reached. Passmore suggests that as a general rule one might have thought that a contested process in which the tribunal controlling the proceedings may make some sort of ruling that has mandatory consequences for a participant that are either penal (such as a prison sentence, a fine or other form of sanction such as a suspension from practice), or otherwise require the participant to do something he or she does not wish to do (such as pay damages, obey an injunction or give an undertaking not to do something), are ones in which the privilege should be available.[120] This must be right and is consistent with the decision of the Court of Appeal in *ENRC*: less significant than the precise stage an investigation by a regulator has reached is whether the client was aware of circumstances meaning that it reasonably contemplated adversarial proceedings ensuing.

Dominant purpose 35.4.3

The dominant purpose for the communication or the production of the relevant document must have been either to obtain information or advice in connection with the litigation or to conduct or assist in the conduct of it. However, in keeping

119 Ibid., at para. 46.

120 *Passmore*, para. 3-095.

See Section 35.4

both with the general language adopted by Lord Edmund-Davies in *Waugh's* case and the overriding rationale underlying litigation privilege, it must be understood as applying to documents and communications produced in many aspects of the litigation process.[121]

The test of 'dominance' is necessarily framed at a certain level of generality. Moreover, it is accepted that in applying it, the court will have to accept that 'human motivation is rarely linear'.[122] A dominant purpose has been described as the ruling, prevailing or most influential purpose – in other words, a purpose that is of greater importance than any other.[123] As a consequence, a practical approach to ascertaining the pre-eminent purpose must necessarily be adopted. In particular, it is not necessary that it be the sole purpose. By the same token, however, it will not suffice if the relevant litigation purpose is merely a secondary, or merely co-equal, purpose.[124] The courts will examine 'purpose' from an objective standpoint,[125] looking at all the relevant evidence, including evidence of the relevant person's subjective purpose.[126] There is sometimes scope for debate as to whether a number of related 'purposes' are properly to be regarded as one overall purpose or as distinct when applying the dominant purpose test. In *Bilta v. RBS*,[127] the various purposes of (1) providing information to Her Majesty's Revenue & Customs (HMRC) in accordance with RBS's duties as a taxpayer, (2) complying with RBS's Codes of Practice and (3) seeking to persuade HMRC to change its mind over a threatened tax assessment, were all held to be effectively subsumed within the dominant purpose of defeating the expected tax assessment. They were said to be part of the inseparable purpose of avoiding litigation if possible, such that the dominant purpose test was satisfied.[128] Similarly, in *ENRC*, there was an issue as to whether it was reasonable to regard ENRC's dominant purpose as being

121 In support of this view, see *Passmore*, para. 3.010.

122 See to this effect *Esso Australia Resources Limited v. The Commissioner of Taxation* (1999) 201 CLR 49, para. 65 (*per* McHugh J), para. 93 (*per* Kirby J).

123 JD Heydon, *Cross on Evidence* (8th Australian edn., 2010), 891.

124 *Waugh v. British Railways Board* [1980] AC 521, 532 (*per* Lord Wilberforce); *Rawlinson & Hunter Trustees SA & Ors v. Akers & Anr* [2014] EWCA Civ 136; *Rawlinson & Hunter Trustees SA & Ors v. Director of the SFO* [2014] EWCA Civ 1129, para. 19.

125 *Price Waterhouse (a firm) v. BCCI Holdings (Luxembourg) SA* [1992] BCLC 583, 591 (*per* Millett J).

126 *Three Rivers No. 5*, para. 35.

127 [2017] EWHC 3535 (Ch).

128 See also *Re Highgrade Traders* [1984] BCLC 151, 173 (*per* Oliver LJ).

to investigate the facts to see what had happened and to deal with compliance and governance issues, or to defend the proceedings that were held to have been in reasonable contemplation at the time. The Court of Appeal held that:

> *[W]here there is a clear threat of a criminal investigation, even at one remove from the specific risks posed by the SFO should it start an investigation, the reason for the investigation of whistle-blower allegations must be brought into the zone where the dominant purpose may be to prevent or deal with litigation.*[129]

Further, the evidence showed that litigation was indeed the dominant purpose of the investigation. The Court's reasoning suggests that, where a party commences a factual investigation related to litigation that is reasonably in contemplation, a court will be inclined to accept that the contemplated litigation is the dominant purpose of that investigation rather than, for example, a purpose of simply establishing the material facts or dealing with compliance issues. It will be different, however, if the party in question is required by a specific policy to conduct an investigation, independent of any risk of litigation: in such a situation, the satisfaction of that policy requirement will be a distinct purpose that prevents the possible litigation from being the dominant purpose.[130]

The Court of Appeal in *ENRC* also considered an argument that the documents in question were not subject to litigation privilege because they were created in a period of co-operative dialogue between the SFO and ENRC and, so the SFO said, with the specific purpose of being shown to the SFO. The Court rejected this argument: the evidence did not support a finding that the documents were created with the specific purpose of being shown to the SFO, despite ENRC having stated to the SFO on a number of occasions that it intended to make 'full and frank disclosure' and to produce its investigation report.

The 'dominant purpose' issue was also considered by the Court of Appeal in *Rawlinson & Hunter Trustees SA v. Akers.*[131] In that case the claimants sought disclosure from the defendants, joint liquidators of certain companies in which the Tchenguiz family had an interest, of five reports prepared by Grant Thornton LLP that, the claimants said, had played a key role in the preparation of, and informed the content of, material placed before a judge in support of the application by the SFO for search warrants of the homes and business premises of Robert and Vincent Tchenguiz. The joint liquidators resisted disclosure on the ground of litigation privilege. Tomlinson LJ explained that the identification of dominant purpose presented the biggest challenge, since 'plainly the first duty of the liquidators was to obtain information simply to establish what if any assets or liabilities existed and what if any steps were open to the liquidators to collect in the assets

129 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, para. 109.

130 *Waugh v. British Railways Board* [1980] AC 521.

131 [2014] EWCA Civ 136.

or to reduce or discharge the liabilities'.[132] The claim to privilege failed in circumstances where the evidence put forward by the joint liquidators in support of that claim failed to grapple with the need to establish which of dual or even multiple purposes was dominant. The dominant purpose must relate to the conduct of actual or contemplated litigation. This includes advice relating to avoidance of that litigation or its settlement once in train.[133]

The law on litigation privilege and dominant purpose seems to have taken a backwards step with the Court of Appeal's decision in *WH Holding v. E20*.[134] The claimants, West Ham, had sued E20 over the number of seats in the London Olympic stadium that West Ham was entitled to use. The decision concerned an application by West Ham for inspection of six emails over which E20 claimed privilege, passing between E20 board members, and between E20 board members and stakeholders. The emails were produced with the dominant purpose of discussing a commercial proposal for the settlement of the related dispute between E20 and West Ham in relation to rights arising under the concession agreement between the parties, which provided for West Ham to use the stadium for its home football matches. The Court of Appeal rejected E20's claim to privilege and held that litigation privilege does not extend to communications concerned with settlement that neither seek advice or information for the purposes of conducting litigation, nor reveal the nature of such advice or information. This is an undoubtedly narrower approach to assessing dominant purpose than was applied in *ENRC*, and adopts a much more restricted concept of the 'conduct' of litigation. The decision is also curious because it generates an inconsistency with the approach of without prejudice privilege. As the first instance judge noted, it gives rise to the anomalous position that a without prejudice offer made by one party to the other in litigation *would not be* before the court in a subsequent case, but any document recording the terms of the offer or its discussion, or the authorisation of the terms and putting of the offer, *would be* open to inspection. What is clear from this decision is that corporates will need to take great care when documenting internal settlement discussions or discussions to avoid litigation, if they wish to avert the risk of any subsequent application for disclosure, and where possible tie those discussions into legal advice so as to obtain the protection of legal advice privilege.

132 Ibid., at para. 15.

133 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791, paras. 102, 118.

134 *WH Holding Limited and West Ham United Football Club Limited v. E20 Stadium LLP* [2018] EWCA Civ 2652.

Common interest privilege 35.5

Common interest privilege (like joint interest privilege, which is not discussed here) can be said to be derivative insofar as it relies on establishing the existence of a primary ground of privilege (whether legal advice or litigation privilege) and then determining the circumstances in which multiple persons become entitled to assert it.

Common interest privilege arises in circumstances where party A voluntarily discloses a document that is privileged in its hands to party B, who has a common interest in the subject matter of the communication, or in the litigation in connection with which the document was produced.[135] Where this occurs, provided disclosure is given in recognition that the parties share a common interest,[136] the document will also be privileged in the hands of party B. Judicial formulation of this principle is found in the following terms:

> *[W]here a communication is produced by or at the instance of one party for the purposes of obtaining legal advice or to assist in the conduct of litigation, then a second party that has a common interest in the subject matter of the communication or the litigation can assert a right of privilege over that communication as against a third party.*[137]

The function of common interest privilege is not simply to prevent party A's privilege from being waived.[138] Where a common interest is made out, it enables party B actually to assert privilege as against a third party. Notwithstanding some terminological confusion, it seems that (unlike joint interest) common interest privilege, properly so-called, does not give party B the right to obtain disclosure of otherwise privileged documents from party A.[139] The rationale of common interest privilege can be explained as follows:

> *It is the communication in confidence to another interested party [in circumstances giving rise to a common interest] that requires the privilege to be available in respect of the document in his hands, whether or not he had the right to require that the document be disclosed to him.*[140]

135 See generally *Thanki*, paras. 6.18 to 6.24.

136 See *Newcrest Mining (WA) Ltd v. Commonwealth of Australia* (1993) 113 ALR 370, 372, Australian Federal Court.

137 *Winterthur Swiss Insurance Company and another v. AG (Manchester) Ltd (in liquidation) and others* [2006] EWHC 839 (Comm), (12 April 2006), (*The TAG Group Litigation*) para. 78 (*per* Aikens J).

138 The fact that, independently of common interest, the disclosure of privileged material to third parties need not involve a broader loss of confidentiality or waiver of privilege is discussed in Section 35.8.

139 For support for this view see *Thanki*, para. 6.21 and *Passmore* para. 6.035. The point appears to have been misunderstood in *The TAG Group Litigation*, where it was held that 'common interest privilege' could operate as a 'sword' to obtain disclosure against party A as well as a 'shield' to deny disclosure to third parties. It seems that that case is therefore best understood as a case of joint interest privilege.

140 Ibid., at 645 (emphasis added).

In other words, common interest privilege is concerned with voluntarily shared privileged information. The aspect of voluntarism is important in understanding the limitations of common interest privilege.[141]

It ought to follow that common interest privilege can be waived by the primary privilege holder.[142] This is the logical conclusion if common interest privilege involves the voluntary disclosure of information. It would be an undue fetter on the primary privilege holder to say that he or she cannot waive privilege without the consent of all those parties with whom he or she has chosen to share his or her advice.

Furthermore, insofar as the proper focus of the doctrine is therefore on the voluntary disclosure of privileged material by party A, it seems that the moment when a common interest must be established is when disclosure occurs.[143]

Although the doctrine is well established, its precise scope continues to be clarified and its requirements must therefore be understood by reference to developments in the recent case law. The doctrine of common (as distinct from joint) interest privilege was first recognised by the Court of Appeal in *Buttes Gas and Oil Co v. Hammer (No. 3)*.[144] A number of statements in that case indicated potential limitations to the doctrine, which, subsequent applications of it have clarified, do not in fact restrict its application.

First, in *Buttes* Lord Denning MR described common interest privilege as being 'a privilege in aid of anticipated litigation'.[145] While this confirms that one core application of the doctrine will be to circumstances in which a common interest arises out of parties' shared concerns regarding prospective litigation (discussed

141 *Commercial Union Assurance Co plc v. Mander* [1996] 2 Lloyd's Rep 640, 647, 648.

142 See, for example, N Andrews, *English Civil Procedure* (2003), para. 27.63. Cf. C Tapper, *Cross and Tapper on Evidence* (12th edn., 2010), 445, where it is stated, without citing any authority, that common interest privilege cannot be waived by one of the parties, without the authority of the other.

143 This point has not received detailed consideration. In *The TAG Group Litigation*, it seems that Aikens J wrongly considered that the relevant time was when the privileged material was first created. However, insofar as he was considering the use of 'common interest' as a 'sword', it appears that his remarks should properly be understood as applying to cases of joint interest. Equally, in *Robert Hitchins Limited v. International Computers Limited* (10 December 1996, CA), Peter Gibson LJ appeared to consider that common interest could not be made out where such an interest did not exist at the time the material first came into being. However, as discussed below, it seems that this did not affect the result in the case, which is probably best seen as a case of common interest privilege.

144 [1981] QB 223, CA. The Court of Appeal's decision was reversed on appeal. However, the House of Lords' ruling (see [1982] AC 888) left unaffected the issue of common interest privilege and the Court of Appeal's decision continues to be seen as the seminal authority for that doctrine.

145 Donaldson LJ (at pp. 251, 252) and Brightman LJ (at p. 267) each spoke of 'contemplated or pending litigation'.

further below), it is now clear that the doctrine is not limited to this context. Hence in *Svenska Handelsbanken v. Sun Alliance and London Insurance plc*,[146] Rix J stated that:

> *It seems to me that if legal advice obtained by one person is passed on to another person for the sake of informing that other person in confidence of legal advice which that person needs to know by reason of a sufficient common interest between them, then it would be contrary to the principle upon which all legal professional privilege is granted to say that the legal advice which was privileged in the hands of the first party should be lost when passed over in confidence to the second party, merely because it was not done in the context of pending or contemplated litigation.*

Support for the fact that common interest privilege can apply outside the context of anticipated litigation can also be found within Commonwealth authority.[147]

The second relevant aspect of *Buttes* concerns whether the parties to the common interest need to have retained the same lawyer (though not under a common retainer). Brightman LJ expressed the doctrine (at p. 267) in terms of the existence of 'a common interest and a common solicitor'. However, it does not appear that either of the other Lords Justice viewed the existence of a common lawyer as a requirement.[148] In some subsequent cases, deference has been paid to Brightman LJ's comments to the extent of suggesting that, while a common lawyer is not required, the commonality of interest requires that the parties could have used the same lawyer.[149] This has also been put in terms of the retention of separate lawyers being a *prima facie* indication that the parties did not have the necessary common interest.[150]

146 [1995] 2 Lloyd's Rep 84 at p. 88.

147 See in particular *Unilateral Investments v. VNZ Acquisitions Ltd* [1993] 1 NZLR 468, 476, 478 (New Zealand High Court).

148 Donaldson LJ in fact pointed out (at pp. 251-252) that, in that particular case, the parties did not initially share a lawyer. Lord Denning also appears to have contemplated that the parties may have separate legal representation. This is implicit to his comments (at p. 243) that the parties may 'have consulted lawyers on the self-same points' and that each 'can collect information for the use of his or the other's legal adviser'.

149 See *Bank of Nova Scotia v. Hellenic Mutual War Risks Association (Bermuda) Ltd (Note)* [1992] 2 Lloyd's Rep 540, 542 (*per* Saville J); *USP Strategies plc v. London General Holdings Limited* [2004] EWHC 373 (Ch), para. 14, *The Times*, 30 April 2004 (*per* Mann J).

150 *Hellenic Mutual War Risks Association (Bermuda) Ltd v. Harrison* [1997] 1 Lloyd's Rep 160, 172 (*per* Rix J).

However, even this limited expression of the need for a putative common lawyer has been criticised in the Australian authorities, in favour of a broader appraisal of common interest.[151] This also now appears to be the approach under English law.[152]

35.6 Without prejudice privilege

The 'without prejudice' rule applies to exclude all negotiations genuinely aimed at settlement from being given in evidence. As with legal professional privilege, no adverse inferences can be drawn against a party invoking the privilege.[153] The rule has two justifications:

- the public policy of encouraging parties to negotiate and settle their disputes out of court; and
- an implied agreement arising out of what is commonly said to be the consequences of offering or agreeing to negotiate without prejudice.[154]

The first justification is the prevailing justification and the second is now doubted and regarded as being at best of limited application.[155] In this context, 'settlement' means 'the avoidance of litigation'.[156] Therefore, the rule is not limited to negotiations aimed at resolving the legal issues between the parties but applies to any negotiations aimed at avoiding or reducing the scope of litigation, irrespective of whether they directly address or seek to resolve the relevant legal issues.

The rule requires the existence of a dispute and an attempt to compromise it.[157] The crucial consideration is whether in the course of negotiations the parties contemplated or might reasonably have contemplated litigation if they could not agree.[158] The use of a 'without prejudice' heading on a letter is not decisive as to whether the privilege applies but does give rise to a rebuttable presumption that

151 See *Bulk Materials (Coal Handling) Services Pty Ltd v. Coal and Allied Operations Pty Ltd* (1988) 13 NSWLR 689, 695 (*per* Giles J); *Network Ten Ltd v. Capital Television Holdings Ltd* (1995) 35 NSWLR 275, 282, Supreme Court of New South Wales (*per* Giles J).

152 In *Formica Ltd v. Export Credits Guarantee Department* [1995] 1 Lloyd's Rep 692, 699 Colman J framed the issue in the following terms: 'The protection by common interest privilege of documents in the hands of someone other than the client must pre-suppose that such third party has a relationship with the client and the transaction in question which, in relation to the advice or other communications, brings that third party within that ambit of confidence which would prevail between the legal adviser and his immediate client . . . the essential question in each case is whether the nature of their mutual interest in the context of their relationship is such that the party to whom the documents are passed receives them subject to a duty of confidence which the law will protect in the interests of justice'.

153 *Reed Executive plc v. Reed Business Information Ltd* [2004] 1 WLR 3026, para. 36.

154 See, for example, *Oceanbulk Shipping & Trading SA v. TMT Asia* [2011] 1 AC 662, paras. 24 and 27.

155 *Barnetson v. Framlington* [2007] 1 WLR 2443, para. 24.

156 *Forster v. Friedland* (CA, 10 November 1992).

157 *Bradford & Bingley plc v. Rashid* [2006] 1 WLR 2066, para. 81.

158 *Barnetson v. Framlingham Group* [2007] 1 WLR 2443 (CA).

the document was intended to be a negotiating document.[159] If a letter is written in reply to a letter written without prejudice or is part of a continuing sequence of negotiations, it will be privileged and cannot be given in evidence without the consent of both parties.[160]

While there was previously some authority to suggest that the without prejudice rule only applied to prevent disclosure of 'admissions', it now appears to be settled that the rule is not limited in this way but that without prejudice discussions as a whole will be protected.[161]

The without prejudice rule is subject to a number of exceptions – it will not apply in the following circumstances:

- *Unambiguous impropriety*: one party may be allowed to give evidence of what the other said or wrote in without prejudice discussions if the exclusion of the evidence would act as a cloak for perjury, blackmail or other 'unambiguous impropriety'.
- *Proof, interpretation and rectification of an agreed settlement*: the rule will not operate to render inadmissible an actual compromise agreement.
- *Misrepresentation, fraud or undue influence*: evidence of without prejudice negotiations is admissible to show that an agreement apparently concluded between the parties during the negotiations should be set aside on the ground of misrepresentation, fraud or undue influence.
- *Estoppel*: where an estoppel founded on a statement made in without prejudice negotiations is alleged, the relevant without prejudice material will be admissible to determine the existence of the estoppel.
- *Reasonableness of mitigating steps*: where there is an issue as to whether a party has acted reasonably to mitigate loss in the conduct and conclusion of negotiations for a settlement the without prejudice material may be examined for that purpose.
- *Delay*: evidence of negotiations may be given to explain delay or apparent acquiescence.[162]

Since the without prejudice privilege belongs to both parties, it cannot be waived without both parties' consent, at least in the context of civil litigation.[163] This is because it is categorised as a joint privilege.[164] However, there is now some limited authority for the proposition that a party to negotiations with a regulatory

159 *Thanki*, paras. 7.13, 7.14.

160 *Dixons Stores Group v. Thames Television* [1992] 1 All ER 349.

161 *Oceanbulk Shipping & Trading v. TMT Asia Limited* [2011] 1 AC 662, para. 27; *Somatra v. Sinclair Roche & Temperley* [2000] 1 WLR 2453, para. 22.

162 See *Thanki*, paras. 7.32 to 7.41.

163 *Walker v. Wilsher* (1889) 23 QBD 335, at 337; *Reed Executive plc v. Reed Business Information Ltd* [2004] 1 WLR 3026, para. 19.

164 D Vaver, 'Without Prejudice Communications – their admissibility and effect' (1974) 9 UBC Law Review 85, at p. 105; Heydon, *Cross on Evidence* (10th edn.) [25350].

authority may unilaterally waive without prejudice privilege in respect of communications with that authority if it subsequently puts the basis of the regulator's decision in issue in civil proceedings.

The law took an unusual and unexpected turn in this direction with the decision of Birss J in *Property Alliance Group Ltd v. Royal Bank of Scotland plc*.[165] The case concerned alleged LIBOR fixing by RBS employees. The claimant, PAG, had purchased interest rate swaps from RBS in 2004–2008 that had been referenced to GBP LIBOR. PAG claimed that it had entered into the swaps in reliance on certain misrepresentations to the effect that RBS was not rigging LIBOR (PAG also relied on alleged implied terms to that effect). In support of its plea that the representations were false, PAG referred to the contents of the final notice issued by the Financial Services Authority (FSA), the predecessor body to the FCA, against RBS, which had found that RBS had manipulated Swiss Franc LIBOR and Japanese Yen LIBOR, but otherwise made no findings in relation to other currency denominations. The FSA final notice had been issued following a settlement reached between RBS and the FSA.

In its defence, RBS admitted that it had manipulated Swiss Franc LIBOR and Japanese Yen LIBOR but denied any wrongdoing in relation to GBP LIBOR. In support of that denial, RBS pleaded: 'For the avoidance of doubt, there have been no regulatory findings of misconduct on the part of RBS in connection with GBP LIBOR.'

PAG sought disclosure of a wide range of documents over which RBS claimed both without prejudice privilege and also legal professional privilege.[166] RBS claimed that communications passing between it and the FSA between December 2012 and January 2013 were subject to without prejudice privilege on the grounds that they recorded negotiations with a view to the settlement announced in February 2013. The FCA wrote a letter in support of RBS's claim to without prejudice privilege on the grounds of public interest.

The judge rejected RBS's right to withhold disclosure of these documents. He held that by pleading in its defence that the regulators had not found any misconduct relating to GBP LIBOR, RBS 'had itself put in issue the basis on which the regulatory findings were made',[167] and as a result RBS had to give disclosure of

165 *Property Alliance Group Ltd v. Royal Bank of Scotland plc.* [2015] EWHC 1557 (Ch).

166 RBS relied on the doctrine of limited waiver. The part of the decision dealing with limited waiver is uncontroversial and consistent with previous authority (see Section 35.8.1).

167 *Property Alliance Group Ltd v. Royal Bank of Scotland plc.* [2015] EWHC 1557 (Ch), para. 94.

the communications.[168] The judge's reasoning, while difficult to discern, appears to have been that communications on which the settlement was based might have been incomplete, mistaken or misleading.[169] As he explained:

> *If the communications on which the Final Notice was based were false, then to allow RBS to rely on what is absent from the Final Notice but at the same time to withhold inspection of those communications would compound the falsehood. That will not do.*[170]

PAG argued that the sort of regulatory context in which the communications between RBS and the FSA took place was not within the without prejudice rule.[171] Birss J rejected the submission that the without prejudice rule was inapplicable, finding that 'the public policy on which the without prejudice rule is based is capable of applying in order to promote the settlement of FCA investigations',[172] but suggested that there is a particular kind of privilege covering settlement negotiations between firms and the FCA (and presumably therefore other regulators) that is 'analogous with' but 'not identical to' without prejudice privilege.[173] Unlike the normal without prejudice rule (where the consent of both parties is required for any waiver of the privilege), this 'analogous' type of without prejudice rule could, according to Birss J, be waived unilaterally by RBS putting the basis on which a final notice was decided in issue in civil proceedings, without the consent of the FCA. This decision is difficult to understand, in particular why the judge decided he needed to fashion a new type of privilege and why this new type of without prejudice privilege is apparently capable of being waived unilaterally.

In the event, RBS applied to amend its defence so as to remove the paragraph that Birss J had held put in issue the basis of the FSA's findings. Birss J held that by doing so RBS could prevent the waiver that had been identified in his earlier judgment from taking place.[174] He held that it was open to a party to decide not to rely on privileged material and therefore amend the relevant pleading, in which case, if the amended pleading was permitted, no waiver would have taken place merely by virtue of having been pleaded previously. Any substantive need for RBS to appeal on the waiver aspect of the first decision of Birss J therefore fell away (and RBS's appeal in relation to other aspects of the decision was in any event settled). The law has accordingly been left in a state of some uncertainty on this topic.

---

168 For the same reason – namely that RBS had 'put in issue' the basis on which regulatory findings were made – Birss J held that RBS was not entitled to withhold from inspection the six privileged documents that it had shared with regulators (see para. 114). This aspect of the decision is discussed below at Section 35.8, but must be wrong.

169 *Property Alliance Group Ltd v. Royal Bank of Scotland plc.* [2015] EWHC 1557 (Ch), para. 92.

170 Ibid., at para. 96.

171 Ibid., at para. 59.

172 Ibid., at para. 87.

173 Ibid., at para. 99.

174 [2015] EWHC 3272 (Ch), para. 69.

35.7 Exceptions to privilege

35.7.1 The crime-fraud exception

See Section 35.7.2

Aside from certain very limited statutory exceptions where privilege may exceptionally be overridden, the principal situation[175] where communications may not be protected by privilege is the crime-fraud exception. In broad terms, this exception provides that there is no privilege in documents or communications that are themselves part of a crime or a fraud, or that seek or give legal advice about how to facilitate the commission of a crime or a fraud. This exception applies to both legal advice privilege and litigation privilege.[176]

It is important to bear in mind the truly exceptional nature of the crime-fraud exception. A court will not lightly deprive a party of the fundamental protection of legal professional privilege,[177] particularly where the privilege is challenged on an interlocutory application.[178] The reason for such caution is plain: once the court determines that the veil of privilege is to be lifted, and that the privileged documents are to be disclosed, there is no return. The holder's right to privilege will have been irretrievably destroyed.

The solicitor need not be involved in the crime or fraud for the exception to apply: the solicitor may be wholly innocent.[179]

Notwithstanding its exceptional nature, it may be that regulators or prosecutors in certain circumstances will wish to challenge a party's claim to privilege on the basis of this exception. To successfully challenge that claim the regulator or prosecutor will need to establish that:

- there was a specific dishonest criminal (i.e., fraudulent) purpose; and
- the privileged material was produced in furtherance of or in preparation for that purpose.[180]

---

175 The Court of Appeal held in the case of *R v. Brown (Edward)* [2016] 1 WLR 1141 that in addition to the fraud/iniquity exception, the normally absolute rule of privilege is capable of further qualification at common law. The Court of Appeal held that it was appropriate, in what was likely to be an extremely narrow band of cases and by way of an additional common law qualification or exception to the inviolable nature of legal professional privilege, to impose a requirement that particular individuals could be present at client–lawyer discussions if there was a real possibility that the discussions were to be misused for a purpose and in a way involving impropriety amounting to an abuse of the privilege that justified interference. In this case, it was appropriate for two nurses to be present with and handcuffed to the appellant, who was in detention in a high security psychiatric hospital, when he consulted with his lawyers because there was reason to think he would otherwise take that opportunity to harm himself or others.

176 *Dubai Aluminium Co Ltd v. Al Alawi* [1999] 1 WLR 1964; *Dubai Bank v. Galadari (No. 6), The Times*, 22 April 1991; *Kuwait Airways Corporation v. Iraqi Airways Company* [2005] 1 WLR 2734.

177 *R v. Cox and Railton* (1884) 14 QBD 153 at 176.

178 *Derby & Co Ltd v. Weldon (No. 7)* [1990] 1 WLR 1156, 1173.

179 *Banque Keyser Ullman SA v. Skandia (UK) Insurance Co. Ltd* [1986] 1 Lloyd's Rep 336, 337.

180 *Butler v. Board of Trade* [1971] 1 Ch 680 at 689C *per* Goff J: 'What has to be shown *prima facie* is not merely that there is a *bona fide* and reasonably tenable charge of crime or fraud but a *prima facie* case that the communications in question were made in preparation for or in furtherance or as part of it.'

As to the evidential burden on the party invoking the exception, there must be some *prima facie* evidence of the crime or fraud; a mere allegation or charge of crime or fraud is not sufficient.[181] In a case where the crime-fraud relied on is one of the issues in the action, the applicable standard is the 'very strong *prima facie* case'; whereas in a case where the issue of fraud is freestanding it may be sufficient to establish a 'strong *prima facie* case'.[182]

There is some debate as to the proper scope of the exception. In the authors' view, being an exceptional principle, the crime-fraud exception applies only in circumstances where the conduct in question amounts to a crime or a fraud (i.e., involving an element of dishonesty).[183] There is, however, some suggestion in some texts and cases that the scope of the exception has been broadened to cases arguably not involving crime or fraud (which has also led to the exception sometimes being termed the 'iniquity exception').[184]

The widening of the exception to encompass conduct falling short of dishonesty is said to emanate from the Court of Appeal's decision in *Barclays Bank v. Eustice*.[185] However, it is doubtful that *Eustice* should be taken as authority for extending the scope of the crime-fraud extension. Though using the language of 'iniquity', in the context of civil proceedings, the Court of Appeal nonetheless was clear that the impugned conduct was a type of fraud (in this case, on the creditors), within the meaning of section 423 of the Insolvency Act 1986. Equally, in *JSC BTA Bank v. Ablyazov*, Popplewell J characterised Mr Ablyazov's conduct in terms of concealment and deceit, namely as dishonest and fraudulent.[186]

Even if, contrary to the above, *Eustice* is understood as having extended the crime-fraud exception to conduct falling short of dishonesty, the basis for such extension is dubious, being based on an authority – *Ventouris v. Mountain*[187] – that was not about the crime-fraud exception at all. Indeed in *McE v. Prison Service of Northern Ireland*,[188] Lord Neuberger left open the question as to whether *Eustice* had been correctly decided.

---

181 *O'Rourke v. Darbishire* [1920] AC 581, 604, 614; *Derby & Co v. Weldon* (No. 7) [1990] 1 WLR 1156, 1166.

182 *Kuwait Airways Corporation v. Iraqi Airways Corp* (No. 6) [2005] 1 WLR 2734, para. 42 (*per* Longmore LJ).

183 *Crescent Farm (Sidcup) Sports Ltd v. Sterling Offices Ltd* [1972] Ch 553, 565 (*per* Lord Goff); *Gamlen Chemical Co (UK) Limited v. Rochem Ltd* (No. 2) 7 December 1979 (CA).

184 A recent example is the decision of the Employment Appeal Tribunal in *X v. Y Limited* ([2018] 8 WLUK 94), 9 August 2018 where Slade J held that legal advice given to a company to the effect that a redundancy programme could be used to dismiss an employee who had made complaints amounted to advice given for the purpose of facilitating an iniquity such that the crime/fraud exception was engaged. This decision is currently under appeal.

185 [1995] 1 WLR 1238.

186 [2014] EWHC 2788 (Comm) at para. 98: 'The evidence establishes at least a very strong *prima facie* case that from the moment Mr Ablyazov engaged Clyde & Co he was bent on a strategy of concealment and deceit in relation to his assets which would involve perjury, forgery and contempt as and when such was required for that purpose.'

187 [1991] 1 WLR 607.

188 [2009] 1 AC 908, para. 109.

A further issue that may arise is whether the dishonest purpose needs to be a purpose of the privilege holder, or whether a dishonest purpose of a third party will suffice. The decision of the House of Lords in *R v. Central Criminal Court, ex p Francis & Francis*,[189] followed in *BBGP Managing General Partner Limited v. Babcock and Brown*,[190] suggests that it may be sufficient if a criminal or dishonest purpose of a third party, not the privilege holder, can be established to the requisite evidential standard. However, those cases do not address the situation where the party claiming privilege is also the party against whom the criminal conduct is alleged.

While these points currently remain untested, it is suggested that the requirements for establishing the crime-fraud exception are likely to present some difficulty for regulators and prosecutors where the privilege holder is a company but where a dishonest or criminal purpose can only be established against certain individuals. In particular, it does not follow that because the criminal or fraudulent purposes of one or more individuals can be established, the necessary fraudulent purpose of the corporate is established. Whether it can be, will depend on complex issues of attribution and the doctrine of identification in the criminal context.

A case of particular interest in the regulatory context is *CITIC Pacific Ltd v. Secretary for Justice and anor*,[191] in which the Hong Kong Court of Appeal considered the application of the crime-fraud exception in the context of alleged fraud and breach of listing rules by a company (CITIC) listed on the Hong Kong Stock Exchange. Hong Kong's Securities and Futures Commission (SFC) had commenced investigating why CITIC had delayed a profit warning in October 2008, during the financial crisis. As part of its investigation into alleged 'defalcation, fraud, misfeasance and other misconduct' on the part of CITIC's management, the SFC sought various documents, including privileged documents, which CITIC subsequently provided to it. The police commenced criminal investigations and CITIC learned that the SFC had passed the privileged documents to the United States Department of Justice for use in the criminal proceedings. CITIC issued an application for an order that the privileged documents be returned on the basis that privilege had been waived for the limited purpose only of the SFC investigation. The application was resisted by the Department of Justice, *inter alia*, on the basis that the documents were created by certain of the persons responsible for the management of CITIC for the purposes of the fraud, such that the crime-fraud exception applied.

The Court of Appeal (reversing the decision of Wright J) found that the crime-fraud exception had not been made out since there needed to be evidence of a fraudulent purpose behind the seeking and obtaining of the advice by the relevant directors of CITIC, which had not been established, for there to be the necessary causal relationship between the advice received and the fraudulent conduct.

189 [1989] 1 AC 346.
190 [2011] Ch 296.
191 [2012] 2 HKLRD 701.

The decision in *CITIC* is instructive in demonstrating a cautious approach by an appellate court to the encroachment of legal professional privilege where the crime-fraud exception is invoked by a prosecuting authority in the context of, and (presumably) in aid of, anticipated criminal proceedings.

Statutory and other exceptions 35.7.2

Previously, the courts did not require a great deal of persuasion that Parliament had intended to override legal professional privilege.[192] That is no longer the case.[193] For example, statutory powers requiring the production of documents would generally be deemed to exclude the right to demand documents subject to legal professional privilege. Any exception to this rule would have to be explicitly supported by primary legislation.[194] Explicit support would require clear language or necessary implication. A necessary implication in this area is not an exercise in interpretation; it is a matter of express language and logic.[195] A necessary implication arises only where the legislative provision would be rendered inoperative or its object largely frustrated in its practical application if the privilege were to prevail.[196] Any curtailment of privilege could only be to the extent reasonably necessary to meet the ends that justify the curtailment.[197]

It appears that there may be a further exception[198] to legal professional privilege where a professional is under investigation by their regulator seeking production of documents over which the professional's client could claim privilege, or the professional wishes to produce the documents to show the regulator that he or she has behaved properly (i.e. 'underlying client-privileged documents' rather than documents over which the professional could claim his or her own privilege).[199] Those documents may be disclosed to the regulator without the client's consent but must not be used against the underlying client, and steps must be taken to

192 See, for example, *R v. Inland Revenue Commissioners, ex p Lorimer* [2000] STC 751.

193 Although *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, HL is regarded as the landmark ruling in this area, *R v. Secretary of State for the Home Department, ex p Daly* [2001] 2 AC 532, paras. 5, 31, HL is of equal significance. These cases applied the more general principle that a statute is generally not intended to override fundamental rights: *R v. Secretary of State for the Home Department, ex p Simms* [2000] 2 AC 115, 131, HL; *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908, paras. 96-97, HL (*per* Lord Carswell).

194 *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 8; *General Mediterranean Holdings SA v. Patel* [2000] 1 WLR 272; *R v. Secretary of State for the Home Department, ex p Daly* [2001] 2 AC 532; *Bowman v. Fels* [2005] 1 WLR 3083, paras. 70 to 91, CA. See also *Baker v. Campbell* (1983) 153 CLR 52.

195 *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 45 (*per* Lord Hobhouse).

196 *Daniels Corporation International Pty Ltd v. Australian Competition and Consumer Commission* (2002) 213 CLR 543, para. 43 (*per* McHugh J).

197 *R v. Secretary of State for the Home Department, ex p Daly* [2001] 2 AC 532, paras. 5 (*per* Lord Bingham) and 31 (*per* Lord Cooke).

198 Though it has been argued that it is not truly an 'exception' because the client's privilege in the relevant material is not infringed.

199 See *Thanki* paras. 4.91 to 4.96.

protect the client's confidential privileged material. The justification for the rule is that either there is no infringement of the client's privilege where the documents may not be used against him or her, or that, if there is an infringement, it is of a technical nature that may be authorised without satisfaction of the usual 'clear language or necessary implication' test.[200] This issue recently arose for consideration in *The Financial Reporting Council Limited v Sports Direct International Plc*.[201] The Financial Reporting Council (FRC), which, among other things, is the regulator for statutory auditors in the United Kingdom, had used its statutory powers to seek the production of certain documents from Sports Direct for the purpose of its investigation into its statutory auditor. Sports Direct withheld the documents on grounds of legal professional privilege and the FRC challenged this, relying on the principle that it, as regulator, was entitled to obtain those documents from Sports Direct, even if they were documents over which Sports Direct had a valid claim to privilege, as long as it did not use those documents against Sports Direct. The judge considered the relevant authorities and, acknowledging that the issue was 'difficult', ultimately agreed with the FRC and ordered that the documents be produced.[202] He summarised the principle as follows:

> *[T]he production of documents to a regulator by a regulated person solely for the purposes of a confidential investigation by the regulator into the conduct of the regulated person is not an infringement of any legal professional privilege of clients of a regulated person in respect of those documents. That being so, in my judgment the same must be true of the production of documents to the regulator by a client.*[203]

However, the principle is not without controversy, and Sports Direct were granted permission by the judge to appeal; it is expected that the question will be revisited by the Court of Appeal in the near future.

The most significant statutory exception in the regulatory context is covert surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA).[204] However, if covert surveillance is likely to result in the acquisition of knowledge of matters subject to legal professional privilege, the appropriate authorisations or approval cannot be made unless there are exceptional and compelling circumstances. Unless that risk can be entirely removed, steps must be taken to ensure that any such information will not be used for the purpose of further investigations or during the course of any subsequent criminal trials.[205]

---

200 *R (Morgan Grenfell & Co Ltd) v. Special Commissioner of Income Tax* [2003] 1 AC 563, para. 32 (*per* Lord Hoffmann).

201 [2019] 2 All ER 974.

202 Ibid., at paras. 57 to 92.

203 Ibid., at para. 84.

204 See *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908. Other limited statutory exceptions are set out in *Thanki*, para. 4.90.

205 *R v. Turner (Elliott Vincent)* [2013] EWCA Crim 643.

Loss of privilege and waiver 35.8

Although privilege, once established, will endure indefinitely, it may be lost, principally in two ways. First, the party entitled to assert privilege may waive the right. This can occur expressly, for example, by choosing to place privileged material before the court. For this purpose, the partial disclosure of a privileged document will usually involve a waiver of privilege in respect of the whole document.[206] Waiver will also occur by necessary implication in certain proceedings (implied waiver). For example, where a client sues a lawyer, the client will be taken impliedly to waive privilege in respect of those documents arising under the retainer subject to dispute.[207]

The second principal circumstance in which privilege will be lost is where there is a loss of confidentiality. As discussed in Section 35.2.1, the confidentiality of the communication or document is a condition precedent to its being privileged. However, the significance of this requirement should not be misunderstood. It is well established that a privileged document does not lose its quality of confidence simply because it is disclosed to persons other than the client and the lawyer. Plainly, if a document has been made available to the general public, all confidence (and with it privilege) will have been lost.[208] However, where privileged material is disclosed to a limited number of third parties in circumstances expressly or impliedly preserving the overall confidentiality as against the rest of the world, privilege will be maintained. This point is well illustrated by an example cited with approval by the English courts:

> *If A shows a privileged document to his six best friends, he will not be able to assert privilege if one of the friends sues him because the document is not confidential as between him and the friend. But the fact six other people have seen it does not prevent him claiming privilege as against the rest of the world.*[209]

206 *Great Atlantic Insurance Co. v. Home Insurance Co.* [1981] 1 WLR 529.

207 See *Paragon Finance v. Freshfields* [1999] 1 WLR 1183. An implied waiver may, however, be limited: see *Eurasian Natural Resources Corporation v. Dechert* [2016] EWCA Civ 375.

208 See (in the general context of an action for breach of confidence) *Attorney-General v. Guardian Newspapers Ltd. (No. 2)* [1990] 1 AC 109, 177, where Sir John Donaldson MR said: 'As a general proposition, that which has no character of confidentiality because it has already been communicated to the world, i.e., made generally available to the relevant public, cannot thereafter be subjected to a right of confidentiality: *O. Mustad & Son v. Dosen* (Note) [1964] 1 WLR 109. However, this will not necessarily be the case if the information has previously only been disclosed to a limited part of that public.'

209 *USP Strategies v. London General Holdings* [2004] EWHC (Ch) 373, para. 19 (*per* Mann J); *Gotha City v. Sotheby's* [1998] 1 WLR 114, CA, para. 119 (*per* Staughton LJ).

It has therefore been accepted that where a client disseminates a record of privileged material, either within its own corporation or to third parties, confidentiality will not necessarily be lost.[210] It is a separate question whether the party to whom the documents are disclosed acquires a right to assert privilege by virtue of a common interest.

See Section 35.5

As noted above in Section 35.6, in *Property Alliance Group Ltd v. Royal Bank of Scotland plc*,[211] it was suggested that privilege can be lost by a party putting something in issue. This aspect of the decision must be wrong: legal professional privilege is absolute unless waived or overridden by statute. There is no balancing act to be carried out with some competing public interest. It may be that the reference to putting something in issue was a confusion with the doctrine of collateral waiver. However, collateral waiver requires some form of 'deployment' of the privileged material, not simply that a relevant matter is put in issue.

See Section 35.8.2

35.8.1 Limited waiver

Limited waiver is achieved where a party discloses a privileged document, or communicates privileged information, to a limited number of third parties in circumstances expressly or impliedly preserving the overall confidentiality of the document or information as against the rest of the world. It is well established that in such circumstances the disclosing party does not lose privilege in the document.[212]

Limited waiver may frequently arise in a regulatory context. In *B v. Auckland District Law Society*,[213] in the course of investigating a complaint against a law firm, certain privileged documents had been handed over to counsel appointed by The Law Society. The letter handing over the documents stated that the documents were made available to counsel for the limited purposes of the investigation and 'on the express basis that in doing so privilege is not waived'. The Law Society sought to use the documents in subsequent disciplinary proceedings brought against the law firm, on the basis that the privilege had been 'let out of the bag'. The Privy Council rejected this submission. Lord Millett held:

> *It does not follow that privilege is waived generally because a privileged document has been disclosed for a limited purpose only . . . . The question is not whether privilege has been waived, but whether it has been lost. It would be unfortunate if it were. It must often be in the interests of the administration of*

210 *Gotha City v. Sotheby's* [1998] 1 WLR 114, CA; *USP Strategies v. London General Holdings* [2004] EWHC (Ch) 373.

211 [2015] EWHC 1557 (Ch).

212 *Gotha City v. Sotheby's* [1998] 1 WLR 114; *Nederlandse Reassurantie Groep Holding NV v. Bacon & Woodrow and others* [1995] 1 All ER 976; *USP Strategies plc v. London General Holdings* [2004] EWHC 373.

213 *B v. Auckland District Law Society* [2003] 2 AC 736.

> *justice that a partial or limited waiver of privilege should be made by a party who would not contemplate anything which might cause privilege to be lost, and it would be most undesirable if the law could not accommodate it.*[214]

There was further development of the limited waiver doctrine in *Berezovsky v. Hine*.[215] Mr Berezovsky's lawyers had sent privileged draft witness statements in relation to Mr Berezovsky's action against Mr Abramovich to solicitors acting for his friend, Mr Patarkatsishvili, in an asylum application as it was thought they might be useful. Mr Patarkatsishvili died and his estate wanted to use the statements in subsequent litigation against Mr Berezovsky. Mann J held that as the statements had been disclosed by Mr Berezovsky's solicitors without any express limitation on their use, it was not open to Mr Berezovksy to prevent their use by the estate against him. The Court of Appeal disagreed. Lord Neuberger MR said that the statements were obviously intended to remain confidential and were disclosed for a limited and defined purpose. In explaining the nature of limited waiver and its scope, Lord Neuberger noted:

> *[W]here privilege is waived, the question whether the waiver was limited, and, if so, the parameters of the limitation, must be determined by reference to all the circumstances of the alleged waiver, and, in particular, what was expressly or impliedly communicated between the person sending, and the person receiving, the documents in question, and what they must or ought reasonably have understood . . . .*[216]

The limited waiver principle was also applied in *CITIC Pacific Ltd v. Secretary for Justice*.[217] The Hong Kong Court of Appeal held that privilege had been waived in favour of the SFC for the purpose of its investigation only, even though at the time of the surrender of the documents to the SFC, CITIC's solicitors provided no written document setting out specific terms as to limitation of the waiver of privilege. It was only several weeks later, in response to an enquiry from the SFC, that CITIC stated in writing what it considered the terms of limitation to have been.

Another instance of the application of the limited waiver doctrine in the regulatory context is the *Property Alliance Group Ltd v. Royal Bank of Scotland plc* decision.[218] RBS claimed privilege over six documents that it had shown to various regulators and the United States Department of Justice and the Attorneys General of several US states. PAG argued that by showing those documents to third parties RBS had waived any privilege in them. The judge disagreed on the basis that the privilege had been waived for a limited purpose only (applying *B v. Auckland*

214 Ibid., at para. 68.
215 *Berezovsky v. Hine* [2011] EWCA Civ 1089.
216 Ibid., at para. 29.
217 [2012] 2 HKLRD 701, discussed at Section 35.7.1.
218 [2015] EWHC 1557 (Ch).

District Law Society and *Berezovsky v. Hine*). Significantly, the judge held that the existence of 'non-waiver' agreements between RBS and the third parties – which recognised by certain 'carve-outs' that the regulator could use the information in a way which could in future destroy the privilege, for example, by publishing the material – did not undermine the limited nature of the waiver. Confidentiality and privilege would continue to be preserved unless some act such as publication, which would destroy the privilege, occurred.[219]

However, while under English law voluntary disclosure to a regulator may not entail a general waiver of privilege, this may be inconsistent with the position in other common law jurisdictions.[220]

In the case of *Dechert v. ENRC*,[221] the Court of Appeal held that the respondent, ENRC, was entitled to have proceedings for the detailed assessment of the bills of its former solicitors, Dechert, held in private and that ENRC had not waived privilege by commencing assessment proceedings. The implied waiver of privilege the application for detailed assessment had entailed was limited, temporary and extended only to the opposing party and to the judge. Gloster LJ remarked that 'the concept of limited waiver is of general application, designed to ensure that the loss of LPP [legal professional privilege] (given its fundamental importance) is limited to that which is necessary to protect other interests.'[222]

Arguments may arise as to the scope of any limited waiver and whether any wider waiver can be inferred from the conduct of the party waiving privilege or the circumstances in which privilege was waived. The scope of the principle of inferred waiver was the subject of consideration by the Divisional Court in *Belhaj v DPP*.[223] *Belhaj* concerned a judicial review of a decision by the Director of Public Prosecutions (DPP) not to prosecute a particular individual. While considering whether to prosecute, privileged material was passed by the government to the Metropolitan Police Service, the Crown Prosecution Service and the DPP under an express limited waiver of privilege. The claimants argued that the waiver must be taken to have extended not only to the police investigation and the decision whether to charge the relevant individual but also to any judicial review proceedings challenging that decision. The Divisional Court rejected that argument, finding that no such wider waiver could be inferred because there was no inevitable or necessary nexus between the decision of the DPP and the subsequent judicial review of the ultimate decision. The key question was whether these were discrete or composite processes. The Court found that the processes were discrete; waiver could not therefore be inferred. There remains scope for argument, on different

219 Ibid., at para. 113.

220 CJQ 324, Case Comment by James Hayton.

221 [2016] 3 Costs LO 327.

222 Ibid., at para. 52.

223 [2018] EWHC 513 (Admin).

facts, as to the extent to which a limited waiver to one person may be inferred to extend to another where that other person requires the relevant document for a purpose that is sufficiently connected to the purpose of the initial limited waiver.[224]

Collateral waiver 35.8.2

In certain circumstances the loss of privilege in a document can lead to waiver of privilege in other material. The rationale for this is one of fairness; the court is concerned to avoid having an incomplete picture of the events in question and to avoid 'cherrypicking' of privileged documents by a party.[225] Lord Bingham CJ commented in *Paragon Finance v. Freshfields* that: 'While there is no rule that a party who waives privilege in relation to one communication is taken to waive privilege in relation to all, a party may not waive privilege in such a partial and selective manner that unfairness or misunderstanding may result.'[226] For this reason it will be more difficult to establish collateral waiver where the initial disclosure was made inadvertently.

The weight of authority suggests that some reliance must be placed on the primary material before any waiver in collateral material can be triggered. Simple disclosure and inspection of the primary material is probably insufficient. The necessary reliance has been said to be deployment of the primary material in court[227] but the approach of the courts to the question of what this means has not always been consistent.[228] Ultimately the touchstone is fairness, and waiver will be found where a party has crossed the line from, for example, merely referring to legal advice to actually relying on that advice in support of its position.[229] In *R v. Papachristos & Kerrison*,[230] an issue arose as to whether Innospec, a company that had pleaded guilty to corruption charges, had waived privilege in certain interview notes by providing a subsequent PowerPoint presentation to the SFO and United States Department of Justice during negotiations, thereby waiving privilege in the presentation. Innospec was not a party to the proceedings and had not sought to deploy any document before the court. It was held that there had been no

224 See, in this regard, *Scottish Lion Insurance v. Goodrich Corporation* [2001] CSUH 18 and *FRC v. Sports Direct International Plc* [2019] 2 All ER 974, paras. 43 to 56.

225 *Nea Karteria Maritime Co v. Atlantic & Great Lakes Steamship Corporation (No. 2)* [1981] Com LR 138; *Paragon Finance v. Freshfields* [1999] 1 WLR 1183.

226 [1999] 1 WLR 1183 at 1188.

227 *Nea Karteria Maritime Co v. Atlantic & Great Lakes Steamship Corporation (No 2)* [1981] Com LR 138; *General Accident Fire and Life Corp v. Tanter* [1984] 1 WLR 100.

228 Compare, for example, *MAC Hotels Limited v. Rider Levett Bucknall UK Limited* [2010] EWHC 767 (TCC) in which HHJ Havelock-Allan QC found that collateral waiver could occur by referring to and relying on privileged material in a witness statement served in support of an (as yet unheard) interlocutory application with the approach of Hobhouse J in *General Accident Fire and Life Corp v. Tanter* [1984] 1 WLR 100, holding that there was no collateral waiver where a privileged note of a conversation was used in cross-examination but before the author of the note was called and before it had been formally admitted in evidence.

229 *Mid-East Sales v. Engineering & Trading Co PVT Ltd* [2014] EWHC 892 (Comm).

230 Unreported Southwark Crown Court, 13 May 2013.

sufficient deployment by Innospec of the notes in the presentation to amount to a collateral waiver of privilege in respect of the notes as opposed to the PowerPoint presentation itself.

The court determined that there had been neither express nor collateral waiver in the interview notes because the waiver that had occurred over the PowerPoint was expressly limited and was in the context of the investigatory stage of the case.

Reliance on part of a document may require disclosure of the whole. While severance may be possible if the document deals with entirely different subject matters, where the document deals with only one subject matter the court may conclude that it is or appears dangerous or misleading to allow a party to deploy part of the document and assert privilege over the remainder.[231]

Once privilege is waived in a particular document, the waiver extends to all documents relating to the same 'transaction', and possibly beyond.[232] The underlying principle applied by the courts is the need to ensure that the evidence adduced by the party claiming privilege is being presented fairly. Hence, in *R v. Secretary of State for Transport ex p Factortame Ltd*, Auld LJ said that:

> *In each case the question for the Court is whether the matters in issue in the document or documents in respect of which partial disclosure has been made are respectively severable so that the partial disclosed material clearly does not bear on matters in issue in respect of which material is withheld. The more confined the issue, for example as to the content of a single document or conversation, the more difficult it is likely to be to withhold, by severance, part of the document or other documents relevant to the document or conversations.*[233]

35.8.3 Inadvertent disclosure and restraining use of privileged documents

The Civil Procedure Rules (CPR) at rule 31.20 provide that, where a party inadvertently allows a privileged document to be inspected, the party who has inspected the document may use it or its contents only with the permission of the court. While the solicitor for one side does not owe a duty of care to the other party,[234] where there is an obvious mistake the solicitor should promptly notify the other party and then, where the client wishes to use the document, make an application under rule 31.20 of the CPR to allow such use. Such use is unlikely to be allowed where the relevant party wishes to use the inadvertently disclosed document as the basis for a new claim, as distinct from the situation where a document is disclosed during litigation.[235]

231 *Great Atlantic v. Home Insurance* [1981] 1 WLR 529.

232 *Thanki*, paras. 5.129 to 5.133.

233 (1997) 9 Admin LR 591 at 599.

234 *Al-Fayed v. Commissioner of Police of the Metropolis* [2002] EWCA Civ 780, para. 16.

235 *Fadairo v. Suit Supply UK Lime Street Ltd* [2014] ICR D11 (EAT) (Singh J).

The question of what is meant by an 'obvious mistake' was considered by the Court of Appeal in *Rawlinson & Hunter Trustees SA & Ors v. Director of the Serious Fraud Office*.[236] Moore-Bick LJ stated that, once it is accepted that the person who inspected a document did not realise that it had been disclosed by mistake, despite being a qualified lawyer, it would be a strong thing for the judge to hold that the mistake was obvious. Further, given the scale of the disclosure in the case and the range of documents involved, general assertions in correspondence that the SFO did not intend to waive privilege were not sufficient to make it obvious that any document arguably privileged must have been disclosed by mistake. On the facts, it was held that it would not have been obvious that the documents at issue in the appeal had been disclosed by mistake.

In *Ford v. FSA*,[237] the claimant established that he had joint interest privilege in two documents provided to the FSA by another party with the benefit of that privilege, and referred to by the FSA in a supplementary investigation report (SIR), without his consent. It followed that the FSA had not been entitled to rely on the content of the communications in the regulatory proceedings. The claimant subsequently sought relief including:

- the quashing of the warning notice issued by the FSA's Regulatory Decisions Committee that referred to the privileged material;
- the destruction of all copies of the privileged documents held by the FSA, together with their permanent deletion from databases and email accounts within the FSA;
- the destruction of all copies of the SIR and warning notices held by the FSA and their permanent deletion from databases and email accounts within the FSA, at least by redaction of the offending passages; and
- the redaction from all hard copy and electronic documents held by the FSA of quotations from or references to the substance of the privileged documents.

Burnett J refused to quash the warning notice, in circumstances where he found that the privileged material formed a very modest part of the overall picture painted by a detailed exposition of the facts and matters on which the FSA relied; it was 'peripheral but not irrelevant'. Rather than equating the FSA's reliance on the privileged material with the public law concept of taking into account an irrelevant matter, the judge held that it was more accurate to consider the error as equivalent to a judicial or administrative body acting, in part, on inadmissible evidence. The warning notice, shorn of the offending references to privileged material, was said to remain a coherent, seamless and powerful document.

236 [2014] EWCA Civ 1129.

237 [2011] EWHC 2583 (Admin) (establishing that two of the documents referred to by the FSA in their supplementary investigation report were subject to joint interest privilege); [2012] EWHC 997 (Admin) (concerning the remedies sought by the claimant in relation to the use of the privileged documents by the FSA).

However, despite the FSA's submission that it would be sufficient to redact the privileged material from the SIR, warning notice and any other documents now to be deployed by the FSA, and to refrain from using or disseminating unredacted copies, Burnett J went further and ordered the FSA to use its best endeavours to identify and destroy such copies (both hard copy and electronic) of the privileged material that existed, together with such copies of the SIR and warning notices. In dealing with the claimant's further request for an order that anyone who had read the privileged documents or was aware of their content should be removed from further involvement in the relevant FSA investigation, the judge held that, while the approach identified in the private law context to the question whether a lawyer in possession of privileged material should be restrained from acting is a useful guide, when the question arises in judicial review proceedings there will necessarily be a public law element in the underlying dispute. The public interest may form an important element in any discretionary decision made in judicial review proceedings. In the particular circumstances of the case, he found that the order sought would be disproportionate and contrary to the public interest.

35.9 Maintaining privilege: practical issues

At the beginning of an investigation litigation may well not yet be in prospect (in which case litigation privilege will not apply) and therefore a corporate may wish to ensure that sensitive communications are, where possible, covered by legal advice privilege. It will be much more difficult to do this in light of the recent decisions in *The RBS Rights Issue Litigation* and *ENRC*, and a corporate embarking on an internal fact-finding investigation with a view to taking legal advice should therefore be aware of the risk that documents created pursuant to that investigation will be disclosable in any subsequent proceedings.

See Section 35.3.2.2

35.9.1 Conducting interviews

The conduct of interviews with potential witnesses is clearly an area of particular sensitivity. Because of the narrow view of who may constitute the 'client' in *Three Rivers No. 5*, as applied in *The RBS Rights Issue Litigation* and *ENRC* (which, while doubted by the Court of Appeal in *ENRC*, still remains the law), regulators or prosecutors may attempt to challenge a claim that the notes of evidence prepared by lawyers at such interviews are protected by legal advice privilege. In a speech to compliance professionals in March 2016, Alun Milford, then General Counsel of the SFO, emphasised the importance the SFO places on witness accounts of relevant events and stated, in this context, that:

> *1. We will view as uncooperative false or exaggerated claims of privilege, and we are prepared to litigate over them: to do otherwise would be to fail in our duty to investigate crime.*
> *2. If a company's assertion of privilege is well-made out, then we will not hold that against the company: to do otherwise would be inconsistent with the substantive protection privilege offers. We will simply judge the question of cooperation in our normal way against our published criteria.*

> *3. By the same token if, notwithstanding the existence of a well-made-out claim to privilege, a company gives up the witness accounts we seek, then we will view that as a significant mark of co-operation: here again, to do otherwise would be inconsistent with the substantive protection privilege offers.*
> *4. For the same reason, we will view as a significant mark of cooperation a company's decision to structure its investigation in such a way as not to attract privilege claims over interviews of witnesses.*[238]

In the first edition of this book, it was suggested that, to preserve privilege when conducting interviews with potential witnesses, in the case of employees, where possible, they should be expressly authorised by the corporate to communicate with the lawyers for the purposes of receiving advice. Such practice would be consistent with the decision of the Singapore Court of Appeal in *Skandinaviska Enskilda Banken v. Asia Pacific Breweries* and would in principle have provided a reasonable ground for asserting privilege on the basis of that decision. The position is much more difficult in light of *The RBS Rights Issue Litigation* and *ENRC* decisions. Following those decisions, and pending any reconsideration of the issue by the Supreme Court, only documents recording communications between the client (i.e., those within the organisation who are authorised to seek advice from, or receive the advice of, the lawyers) and the lawyers will be protected by legal advice privilege. That said, it seems likely that a corporate entity may nevertheless soon seek to maintain legal advice privilege over interview notes (notwithstanding that such a claim to privilege would likely be successfully challenged at a first instance) with the benefit of the Court of Appeal's comments in *ENRC* about the unworkability of a narrow definition of 'client' in the corporate context.[239] However, until such a challenge (and clarification from the Supreme Court), notes of interviews with other employees or ex-employees of the client organisation, whether taken by employees or by the lawyers, will be potentially disclosable in any subsequent proceedings, unless they can be said to form part of the lawyers' working papers. As to that, the decisions in *The RBS Rights Issue Litigation* and, at first instance, *ENRC* suggest that it will be necessary to establish in evidence that the notes, if disclosed, would betray the tenor of the legal advice. It may therefore be tempting for the lawyers to ensure that any notes recording factual information obtained from employees and ex-employees are produced so that they contain the solicitor's commentary and advice and are not merely a recitation of facts provided by the interviewee.

See Section 35.4.2

Of course, all interviews conducted for the dominant purpose of anticipated litigation ought to attract litigation privilege.

See Section 35.4.3

238 Alun Milford, General Counsel, SFO, Speech at the European Compliance and Ethics Institute, Prague, 29 March 2016.

239 In such a case it would seem very likely that a leap-frog certificate would be granted to enable the issue to be determined by the Supreme Court, bypassing the Court of Appeal.

Where a corporation under investigation provides oral summaries of otherwise privileged interviews to a regulator or prosecutor, it is likely that this would be held to amount to a limited waiver in respect of matters communicated to the regulator or prosecutor because the information is provided for the limited purpose of the investigation.

See Section 35.8.1

35.9.2 Ensuring that any waiver is limited

It is clearly very valuable for a regulated entity to be able to waive privilege vis-à-vis the regulator for a particular purpose (e.g., in connection with a specific investigation) but without waiving it more generally. As noted above in Section 35.8.1, in *ENRC v. Dechert* the Court of Appeal has confirmed that the concept of limited waiver is of general application, designed to ensure that the loss of legal professional privilege (given its fundamental importance) is limited to that which is necessary to protect other interests.[240]

Although it may be possible for a regulated entity to contend that waiver of privilege was impliedly, if not expressly, limited (having regard to all the circumstances of the waiver), the safest course will always be to make clear at the time of disclosure that waiver is for a limited purpose only and confidentiality is otherwise being maintained.

However, as noted above, while it may be possible to achieve a limited waiver under English law, the waiver may not be so regarded in other jurisdictions.

35.9.3 Redaction of documents

Where only part or parts of a document are privileged, the appropriate procedure (assuming the privilege holder wishes to maintain privilege) is to disclose the document but redacting the privileged parts. Disclosure of a redacted document will not give rise to a waiver of privilege in respect of the redacted parts.[241] Disclosure of a redacted document in this way should be distinguished from deployment of a redacted document in court. In the latter circumstance, reliance on the unprivileged part of a document may give rise to collateral waiver in respect of the privileged part, where both parts deal with the same subject matter.

See Section 35.2

Where there is a dispute as to the justification for a redaction, the court may inspect the relevant document. In civil proceedings, the court's power to inspect documents to resolve an application for specific disclosure is found in the CPR at rule 31.19(6). Previously, it had been held that an order for inspection by the court is usually regarded as a solution of last resort and should not be undertaken unless the court considers that there is credible evidence that those claiming privilege have either misunderstood their duty, or are not to be trusted with the decision, or there is no reasonably practical alternative.[242] A recent Court of Appeal decision has suggested that the hurdle to be surmounted before inspection

240 [2016] 1 WLR 4205, para. 52 (*per* Gloster LJ).

241 *GE Capital Corporate Finance Group v. Bankers Trust Co* [1995] 1 WLR 172.

242 *West London Pipeline v. Total UK* [2008] 2 CLC 258, para. 86(4)(c).

is ordered is not as stringent, holding that the Court has a general discretion to inspect documents, but that it should nevertheless be cautious before exercising that discretion.[243]

In the criminal context, if the prosecution is asserting public interest immunity in order not to disclose material, there is a defined route to follow under Criminal Procedure and Investigations Act 1996 (CPIA 1996) and the Criminal Procedural Rules (CrimPR) at rule 15.3.

The ability of the defence to challenge the adequacy of prosecution disclosure is provided for under section 8 of the CPIA 1996 and rule 15.5 of the CrimPR, after service of the defence case statement. The court may order disclosure of further material if the defence can demonstrate that the prosecution has that material and is required to disclose it in accordance with the CPIA 1996. A criminal court also has inherent jurisdiction to ensure a fair trial and, in the event of a dispute over the justification for a redaction, a judge can always review the material if he or she considers it appropriate.

Substantiating a claim to privilege if challenged 35.9.4

If a claim to privilege is challenged by an investigating authority or regulator, and the matter comes before the court, it will be necessary for the party claiming privilege to provide evidence to substantiate its claim. The principles to be applied in assessing that evidence were set out by Beatson J in *West London Pipeline v. Total UK*.[244] The judge explained that an affidavit claiming privilege 'should be specific enough to show something of the deponent's analysis of the documents or, in the case of a claim to litigation privilege, the purpose for which they were created. It is desirable that they should refer to such contemporary material as it is possible to do so without making disclosure of the very matters that the claim for privilege is designed to protect.'[245]

While these principles are well established, their application may in some instances be controversial. In *ENRC* the first-instance court did not consider that the evidential burden has been satisfied.[246] In particular, Andrews J was unimpressed by the explanation that had been given as to why evidence had to be

243 *WH Holding Limited and West Ham United Football Club Limited v. E20 Stadium LLP* [2018] EWCA Civ 2652 at para. 40.

244 [2008] 2 CLC 258. Although note, as set out above, the Court of Appeal's disapproval in *WH Holding Limited and West Ham United Football Club Limited v. E20 Stadium LLP* [2018] EWCA Civ 2652 of Beatson J's approach to inspection.

245 Ibid., at para. 53. It was also noted (at paras. 65, 86) that an affidavit is generally to be treated as conclusive unless it appears that the deponent has mischaracterised documents or it is reasonably certain from the evidence before the court that it is incorrect or incomplete on material points.

246 Similarly, in *The RBS Rights Issue Litigation*, Hildyard J did not consider that the evidence adduced by RBS was sufficient to make good RBS's claim that the interview notes comprised the lawyers' working papers as the evidence amounted to no more than a 'conclusory assertion'. As in *ENRC,* it is not easy to see what further evidence RBS could have adduced in support of the contention that disclosure of the notes would betray the trend of legal advice, without revealing the very matters over which RBS was seeking to claim privilege.

adduced in the form of a witness statement from ENRC's solicitors rather than in the form of direct evidence from individuals at ENRC responsible for giving instructions to their lawyers. (The explanation for this was that the senior officers and employees at ENRC were not willing to give evidence in circumstances where they were or might become suspects in the SFO's investigation, without assurances that the SFO would not pursue cross-examination of those witnesses in the proceedings or seek to refer to that evidence against that witness or against ENRC in any subsequent criminal proceedings. The SFO was unwilling to give any such assurances.) This approach seemed to prejudice a corporate claiming privilege in a criminal context given that necessarily the company can only give direct evidence through its directors and employees who may themselves be at risk of investigation and prosecution.

In rejecting ENRC's evidence, Andrews J was also influenced by what she perceived to be an absence of contemporaneous documents to support the claim. In particular, she commented that she had not been shown any records of discussions either at board level or within any group at ENRC that might have shed light on what ENRC contemplated, and why they contemplated it.[247] She therefore considered that for the purposes of the claim to litigation privilege, ENRC had failed to establish a reasonable anticipation of litigation.

The Court of Appeal in *ENRC* was critical of this approach and of the judge's failure to have proper regard to the unchallenged evidence of ENRC (put forward primarily by its solicitor) and the contemporaneous documents.[248] Following this decision, it appears that a corporate claiming privilege will not be prejudiced if, in light of the risk of investigation and prosecution of the individual directors and employees who might otherwise give evidence, it is left with no real choice but to give evidence through its lawyers.

Furthermore, the Court of Appeal's decision in *ENRC* confirms the proper approach explained in *West London Pipeline*, namely that the evidence in a witness statement or affidavit should be accepted unless there is good reason (e.g., the existence of contradictory contemporaneous documents) to think that the evidence is incorrect.

35.9.5 Use of independent counsel

Where there is a potential dispute concerning the application of privilege, it is reasonably common for independent counsel to be appointed to review the relevant documents. Such counsel would then be prevented from acting for either side of the relevant dispute. An appointment may be made by the court or can be made more informally by the parties themselves. This process is, for example, frequently adopted by the SFO, although parties should always ensure the genuine independence of any counsel appointed.

247 *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2017] 1 WLR 4205 at para. 46.

248 See, in particular, *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Limited* [2019] 1 WLR 791 at paras. 92, 93.

In *R (McKenzie) v. Director of the Serious Fraud Office*,[249] the court was required to consider the procedures adopted by the SFO for dealing with potentially privileged material embedded in electronic devices seized using statutory powers or produced in response to a notice. The applicant complained that the SFO procedure was unlawful in using in-house technical staff to conduct an electronic search of the content of seized devices by reference to search terms for the purpose of isolating potentially privileged material for subsequent review by independent counsel. It was argued that this initial exercise should be contracted out by the SFO to independent IT specialists, despite the SFO having detailed procedures in place to ensure, in so far as possible, that its investigators would not gain access to any potentially privileged material before it had been reviewed by independent counsel. The applicant contended that the involvement of in-house SFO IT specialists and the uploading of the digital material, including the potentially privileged material embedded within it, onto the SFO's digital review system unnecessarily exposed the person to whom privilege attached to an avoidable risk that privileged material may come to the knowledge of the SFO and be used to his disadvantage.

The applicant in *McKenzie* argued that the same approach should apply when an investigating body lawfully comes into possession of potentially privileged material as applies to a solicitor in relation to privileged material relating to a former client. The investigating body must satisfy the court with convincing evidence that there is no real risk of the privileged material being disclosed to an investigator. The court disagreed, finding that it would not be appropriate to apply the same reasoning to the relationship between a criminal investigating body and the subject of its investigation as applies in relation to a solicitor and former client. In the case of an investigating body, there is no fiduciary relationship and the body is exercising statutory powers for the public good in the investigation of suspected crime. It would therefore be imposing too onerous an obligation on the SFO to require it to demonstrate that there could be no real risk of the privileged material being read by anyone involved in the investigation; instead, the seizing authority has a duty to devise and operate a system to isolate potentially privileged material from bulk material lawfully in its possession that can reasonably be expected to ensure that such material will not be read by members of the investigative team before it has been reviewed by an independent lawyer to establish whether privilege exists. There should also be clear guidance in place so that, if an investigator does by mischance read privileged material, that fact is recorded and reported, the potential conflict recognised and steps taken to prevent privileged information being deployed in the investigation. On the facts, the SFO procedure was held to satisfy these requirements.

249 [2016] EWHC 102 (Admin).

36

Privilege: The US Perspective

Richard M Strassberg and Meghan K Spillane[1]

36.1 Privilege in law enforcement investigations

36.1.1 Attorney–client privilege

The attorney–client privilege is recognised in the United States as 'the oldest of the privileges for confidential communications known to the common law'.[2] It is viewed as serving a crucial function in 'encourag[ing] full and frank communication between attorneys and their clients' and thereby promoting 'the observance of law and administration of justice'.[3] The attorney–client privilege protects information shared between a lawyer and the client, where the information is (1) a communication, (2) made in confidence, (3) between a person who is, or is about to become, a client (4) and a lawyer (5) for the purpose of obtaining legal advice or assistance.[4] Attorney–client privileged communications may take many forms, from oral communications, to emails, to text messages, so long as each communication is undertaken in confidence for the purpose of seeking or rendering legal advice.[5] Once the privilege is created, the privilege continues, and may be invoked at any time (unless it has been waived or is otherwise subject to an exception), even following the termination of the attorney–client relationship or the death of the client.[6]

---

1 Richard M Strassberg and Meghan K Spillane are partners at Goodwin.

2 *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

3 Id. at 392.

4 See, e.g., *In re Richard, Inc.*, 68 F.3d 38, 39-40 (2d Cir. 1995).

5 See, e.g., *Haines v. Liggett Grp.*, 975 F.2d 81, 90 (3d Cir. 1992) (explaining that privilege extends to verbal statements, documents and tangible objects conveyed in confidence for the purpose of legal advice).

6 David M. Greenwald & Michele L. Slachetka, Protecting Confidential Legal Information, Jenner & Block LLP 104 (2015), https://jenner.com/system/assets/assets/8948/original/2015Jenner_

In *Upjohn Co. v. United States*,[7] the United States Supreme Court held that a company's attorney–client privilege extends to company counsel's communications with employees in certain prescribed circumstances.[8] Rather than providing a simple objective test, the *Upjohn* court instead established five factors to guide courts in determining whether the company's privilege should extend to counsel's communications with its employees: (1) whether the communications were made by employees at the direction of superior officers of the company for the purpose of obtaining legal advice; (2) whether the communications contained information necessary for counsel to render legal advice, which was not otherwise available from 'control group' management; (3) whether the matters communicated were within the scope of the employee's corporate duties; (4) whether the employee knew that the communications were for the purpose of the company obtaining legal advice; and (5) whether the communications were ordered to be kept confidential by the employee's superiors, including that the communications were considered confidential at the time and kept confidential subsequent to the interview.[9] When these elements are established, courts generally consider communications between company counsel and an employee to be within the scope of the company's attorney–client privilege.[10]

See Section 36.3.1

While the privilege provides broad protection for confidential communications among those within the attorney–client relationship, disclosing the contents of these communications to a third party outside the scope of the protection – such as a government agency – may result in a waiver of the applicable privilege.

See Section 36.4

Crime-fraud exception 36.1.1.1

The attorney–client privilege does not offer an absolute protection for all of a lawyer's communications with the client. An important exclusion is the crime-fraud exception, which removes the protection of the attorney–client privilege for communications concerning contemplated or continuing illegal or fraudulent acts.[11]

26BlockAttorney–clientPrivilegeHandbook.pdf (citing *United States v. United Shoe Mach. Corp.*, 89 F. Supp. 357, 358 (D. Mass. 1950); *Swidler & Berlin v. United States*, 524 U.S. 399, 405-06 (1998)).

7 449 U.S. 383 (1981).

8 Id.

9 Id. at 394-96. While the majority of jurisdictions have adopted *Upjohn*'s approach, some states employ other tests to determine if conversations with an employee are covered by the company's privilege. See, e.g., *Motorola, Inc. v. Lemko Corp.*, No. 08 C 5427, 2010 WL 2179170, at *1-2 (N.D. Ill. 1 June 2010) (noting that Illinois continues to apply the control group test and assess privilege questions accordingly).

10 To ensure that the employee understands the purpose of the interview, the expectation of confidentiality, and the scope of the attorney–client privilege, company counsel typically begins each meeting with a company employee by providing a summary of these factors, known as an '*Upjohn* warning'.

11 See, e.g., *United States v. Zolin*, 491 U.S. 554, 563 (1989) (explaining that the crime-fraud exception 'assure[s] that the seal of secrecy between lawyer and client does not extend to communications made for the purpose of getting advice for the commission of a fraud or crime') (citation omitted); *Clark v. United States*, 289 U.S. 1, 15 (1933); *In re Antitrust Grand Jury*,

After a party has invoked the attorney–client privilege, the person seeking to abrogate the privilege under this exception has the burden of making a *prima facie* case that (1) the client was committing or intending to commit a crime or fraud and (2) the attorney–client communications at issue were in furtherance of that alleged crime or fraud.[12] Significantly, for the exception to be applicable, the party need not show that the alleged crime or fraud was actually completed, only that the crime or fraud was the objective of the communication.[13] Further, the party need not show that the attorney was aware of the alleged fraud or misconduct. In fact, the attorney's knowledge or ignorance of the crime is irrelevant. Instead, courts look to the client's intent or objective in the subject communication.[14] As the Supreme Court stated in *Clark v. United States*, 'A client who consults an attorney for advice that will serve him in the commission of a fraud will have no help from the law. He must let the truth be told.'[15]

For example, in the case of *United States v. Gorski*,[16] a defendant was indicted for making fraudulent representations related to the ownership and control of his company when bidding on government contracts.[17] The government alleged that the defendant fraudulently represented that his business qualified as a service-disabled veteran-owned small business entity,[18] and also sought to restructure his company through backdated documents to give the appearance of compliance with ownership regulations.[19] In response to a government subpoena for access to communications between the defendant and his lawyer regarding the ownership and restructuring efforts, the trial court held an *in camera* review and *ex parte* hearing, and determined that the requested documents should be produced under the crime-fraud exception.[20] On appeal, the First Circuit upheld the trial court's ruling, finding that (1) the indictment provided a reasonable basis to believe that the defendant was engaged in criminal or fraudulent activity and

805 F.2d 155, 162 (6th Cir. 1986); *In re Grand Jury Subpoenas Duces Tecum*, 773 F.2d 204, 206 (8th Cir. 1985); *United States v. Horvath*, 731 F.2d 557, 562 (8th Cir. 1984).

12 See *In re Grand Jury Subpoena*, 223 F.3d 213, 217 (3d Cir. 2000); *In re Sealed Case*, 754 F.2d 395, 399 (D.C. Cir. 1985).

13 See *In re Grand Jury Subpoena Duces Tecum*, 731 F.2d 1032, 1039 (2d Cir. 1984).

14 See, e.g., *United States v. Weingold*, 69 Fed. Appx. 575, 578 (3d Cir. 2003) (noting that the privilege may be disregarded even if the lawyer is innocent in relation to the fraudulent scheme); *In re Grand Jury Proceedings*, 87 F.3d 377, 381-82 (9th Cir. 1996). ('[I]t is the client's knowledge and intentions that are of paramount concern to the application of the crime-fraud exception; the attorney need know nothing about the client's ongoing or planned illicit activity. . . .'); *In re Sealed Case*, 754 F.2d at 402 ('[A]n attorney's ignorance of his client's misconduct will not shelter that client from the consequences of his own wrongdoing.'); *Horvath*, 731 F.2d at 562. ('Whether the attorney is ignorant of the client's purpose is irrelevant.')

15 289 U.S. 15 (1933).

16 807 F.3d 451 (1st Cir. 2015).

17 Id. at 455-56.

18 By representing his company as being a service-disabled-veteran-owned small business, the defendant was awarded certain set-aside or sole source government contracts for which he would not have otherwise been eligible. See 13 C.F.R. §125.8-125.10.

19 Id.

20 Id. at 456-57.

(2) there was a reasonable basis to believe that the attorney–client communications 'were intended by the client to facilitate or conceal the criminal or fraudulent activity'.[21] In so ruling, the court specifically noted that the crime-fraud exception does not require – and therefore does not reflect – any finding on the ultimate question as to whether the defendant acted wrongfully, nor does it bear on the conduct or intent of the lawyers involved.[22]

The crime-fraud exception has also been found to apply because of an attorney's misconduct, even if the client is found to be innocent of any wrongdoing.[23] The exception does not apply to attorney–client communications that reflect the solicitation or provision of legal advice concerning crimes or frauds that occurred in the past; such attorney–client communications remain protected,[24] unless the communications are made for the purpose of covering up past misconduct or obstructing justice.[25] Attorney–client communications reflecting advice about the legality of a client's intended course of conduct are likewise protected as privileged.[26] Finally, communications where an attorney dissuades or prevents the

21 Id. at 460-61 (internal quotation marks omitted).

22 Id. at 462.

23 See *Drummond Co. v. Conrad & Scherer, LLP*, 885 F.3d 1324, 1338 (11th Cir. 2018) (applying a balancing test 'to weigh the client's interest in secrecy against the reasons for disclosure').

24 See, e.g., *Zolin*, 491 U.S. at 562 (explaining that the crime-fraud exception applies 'where the desired advice refers not to prior wrongdoing, but to future wrongdoing') (citation omitted).

25 See, e.g., *In re Grand Jury Proceedings*, 102 F.3d 748, 751 (4th Cir. 1996) (noting that the crime-fraud exception includes 'concealment or cover-up of [the client's] criminal or fraudulent activities'); *United States v. Laurins*, 857 F.2d 529, 540 (9th Cir. 1988). ('Obstruction of justice is an offense serious enough to defeat the privilege.')

26 If a client seeks advice from counsel about the legality of a course of conduct and then relies to his or her detriment on that advice in taking action later determined to be unlawful, the client may choose to assert an 'advice of counsel' defence to demonstrate a lack of wrongful intent. The client generally must show (1) full disclosure of all material facts to the attorney before seeking advice; and (2) actual reliance on counsel's advice in the good faith belief that the conduct was legal. See, e.g., *United States v. West*, 392 F. 3d 450, 457 (D.C. Cir. 2004). Invoking the 'advice of counsel' defence generally waives the attorney–client privilege protecting the underlying communications with counsel related to the advice, since the client is putting the contents of those communications at issue. See, e.g., *Chevron Corp. v. Pennzoil Co.*, 974 F.2d 1156, 1162-63 (9th Cir. 1992).

There are limits to the ability of an individual employee to assert the advice-of-counsel defence where the client is the company, rather than the individual. In the civil context, for example, if the corporation controls the privilege over the attorney advice at issue, at least one court has found that the company may refuse to waive that privilege on behalf of the individual employee, even if the disclosure would amount to a complete defence of the individual. See *United States v. Wells Fargo Bank, N.A.*, 132 F. Supp. 3d 558, 566 (S.D.N.Y. 2015). In the criminal context, however, there appears to be split authority as to whether an individual's right to present his defence may trump the company's interest in preserving the privilege. Compare *United States v. Grace,* 439 F. Supp.2d 1125, 1142 (D. Mont. 2006) (finding that such evidence may be 'of such probative and exculpatory value as to compel the admission of the evidence over [the company's] objection as the attorney–client privilege holder.'), with *Wells Fargo Bank, N.A.,* 132 F. Supp 3d at 562-63 (suggesting that the Supreme Court's rejection of a 'balancing test' for attorney–client privilege in *Swidler & Berlin v. United States,* 524 U.S. 399 (1998), may extend to criminal cases as well).

client from engaging in further illegal conduct are also protected; such communications are viewed as serving an important purpose in the administration of justice by promoting legal conduct.[27]

36.1.1.2 Derivative claim exception

Another exception to a company's assertion of attorney–client privilege arises from the case of *Garner v. Wolfinbarger,*[28] where shareholders filed a derivative suit against a company, charging management with fraud and seeking discovery of privileged communications between management and in-house counsel.[29] In an effort to balance the importance of maintaining the confidentiality of attorney communications with the need to keep the shareholders informed of matters affecting the corporation, the Fifth Circuit created an exception to attorney–client privilege, which has become known as the *Garner* doctrine. The doctrine permits a company's shareholders who are suing on behalf of the corporation to bypass the company's attorney–client privilege upon a showing of 'good cause', based on a nine-factor analysis.[30] The *Garner* doctrine has been recognised as creating a shareholder fiduciary exception to attorney–client privilege, though the doctrine is not universally accepted by the courts.[31] Furthermore, whether the Garner doctrine's 'good cause' exception extends to attorney work product also remains unsettled.[32]

---

27 See, e.g., *In re Grand Jury Investigation*, 772 N.E.2d 9, 21-22 (Mass. 2002).

28 430 F.2d 1093 (5th Cir. 1970), cert. denied, 401 U.S. 974, 91 S. Ct. 1991, 28 L.Ed.2d 323 (1971).

29 Id. at 1095-96.

30 Id. at 1104 (outlining the 'indicia' of the presence or absence of 'good cause' to include: (1) the number of shareholders and the percentage of stock they represent; (2) the *bona fides* of the shareholders; (3) the nature of the shareholders' claim and whether it is obviously colourable; (4) the apparent necessity and desirability of the shareholders having the information and the availability of it from other sources; (5) whether, if the shareholders' claim is of wrongful action by the corporation, it is of action criminal, or illegal but not criminal, or of doubtful legality; (6) whether the communications related to past or to prospective actions; (7) whether the communication is of advice concerning the litigation itself; (8) the extent to which the communication is identified versus the extent to which the shareholders are blindly fishing; and (9) the risk of revelation of trade secrets or other information in whose confidentiality the corporation has an interest for independent reasons).

31 See, e.g., *Wal-Mart Stores Inc. v. Indiana Elec. Workers Pension Fund Trust IBEW*, 95 A.3d 1264, 1278-80 (Del. 2014) (adopting the 'fiduciary' exception outlined in *Garner* and finding that plaintiff shareholders who make a showing of good cause can inspect documents concerning a corporation's internal investigation, even if those documents were otherwise governed by the attorney–client privilege); *NAMA Holdings, LLC v. Greenberg Traurig, LLP,* 18 N.Y.S.3d 1, 9-10 (N.Y. App. Div. 2015) (adopting the fiduciary exception test enunciated in *Garner* and rejecting the corporation's argument that the fiduciary exception is inapplicable once its shareholder-plaintiffs become adverse to the company); but see *Hoiles v. Superior Court,* 204 Cal. Rptr. 111, 115 (Cal. Ct. App. 1984) (rejecting *Garner* and holding that California does not afford an 'extraordinary avenue . . . to petitioners to pierce the privilege in their capacity as shareholders'); Pittsburgh History & Landmarks Foundation v. Zeigler, 200 A.3d 58 (Pa. 2019) (rejecting the 'good cause' standard articulated in *Garner* as inconsistent with the basic tenets of attorney–client privilege law because it introduced uncertainty into the application of the privilege).

32 See *Murphy v. Gorman*, 271 F.R.D. 296, 311-313 (D.N.M. 2010) (collecting cases).

While the *Garner* case arose in the context of a shareholder derivative suit, its principles apply more broadly to other situations where a company owes a fiduciary duty to the party seeking to abrogate the privilege.[33] In a case where, for example, a special litigation committee has undergone an internal investigation into the merits of such a claim, derivative plaintiffs might seek access to the investigation materials under *Garner*. To protect attorney–client privileged communications in this context from the risk of later disclosure to the company's shareholders, counsel should diligently mark any written legal advice as attorney–client privileged and, where applicable, attorney work-product. Counsel should also seek to avoid situations where the only evidence of an unprivileged fact is a privileged writing, as this may support a shareholder's 'good cause' to pierce the attorney–client privilege to discover that underlying fact.

Attorney work-product 36.1.2

In the United States, the doctrine of 'attorney work-product' also protects from disclosure certain documents and other materials prepared in anticipation of litigation or for trial. Although such work-product is most commonly prepared by an attorney, work-product protection may extend to materials prepared in anticipation of litigation by certain third parties at the attorney's direction, including materials prepared by the client.[34] But while the work-product doctrine offers certain protections for an attorney's impressions, opinions and legal conclusions, such documents are not considered 'privileged' like attorney–client communications, but instead are afforded a qualified protection from discovery.[35]

In the seminal case of *Hickman v. Taylor*,[36] the United States Supreme Court formally recognised the attorney work-product doctrine, establishing the scope of the protection to include materials prepared in anticipation of litigation.[37] The *Hickman* court also qualified this work-product protection by finding that, upon a showing of good cause, an adversary could obtain discovery of documents containing 'factual work product'.[38] The Court recognised that substantially greater

33 See, e.g., *Buttonwood Tree Value Partners, L.P. v. R.L. Polk & Co., Inc.*, Civil Action No. 9250-VCG, 2018 WL 346036, at *3 (Del. Ch. 10 January 2018) (suggesting that *Garner* could apply to situations in which former stockholders assert a direct claim against a corporation that a class of shareholders was injured by corporate fiduciaries); but see *Morris v. Spectra Energy Partners (DE) GP, LP*, Civil Action No. 12110-VCG, 2018 WL 2095241, at *5 (Del. Ch. 7 May 2018) (holding that the *Garner* exception does not apply to a limited partnership that has eliminated common-law fiduciary duties, reasoning that *Garner*'s applicability depends on the existence of a mutuality of interest between parties).

34 *Hertzberg v. Veneman*, 273 F. Supp. 2d 67, 76 (D.D.C. 2003).

35 See Fed. R. Civ. P. 26(b)(3).

36 329 U.S. 495 (1947).

37 Id. at 511.

38 Id. at 511-12.

– if not absolute – work-product protection should be given to documents that reflect the attorney's legal theories, strategy, assessments and mental impressions (opinion work-product).[39]

In *United States v. Nobles*,[40] the Supreme Court extended the work-product doctrine beyond the scope of materials created by counsel, recognising that attorneys often rely on the assistance of investigators and other agents in preparation for trial. The Court found that it is 'necessary that the [attorney work-product] doctrine protect material prepared by agents for the attorney as well as those prepared by the attorney himself.'[41] Following the Supreme Court's guidance in *Nobles*, work-product protection is understood to be extended to material prepared 'by or for [a] party's representative' as long as the agent is assisting in preparing for litigation and working at the direction of the attorney.[42]

The modern federal work-product doctrine is codified in Rule 26(b)(3) of the Federal Rules of Civil Procedure (the Federal Rules), and stands in line with the Supreme Court's guidance in *Hickman* and *Nobles*. In particular, Rule 26(b)(3) eliminates the distinction between attorney work-product and non-attorney work-product, focusing on whether the materials were prepared in anticipation of litigation or trial.[43] Further, Rule 26(b)(3) preserves work-product protections unless the party seeking discovery has a 'substantial need' for the materials in the preparation of the party's case and the party is unable without 'undue hardship' to obtain the 'substantial equivalent' of the materials by other means.[44]

While the attorney work-product doctrine offers a qualified protection for documents created in anticipation of litigation, disclosing the contents of such documents to a third party outside of the attorney–client relationship (such as a government agency) may result in a waiver of this protection.[45] In addition, courts will examine the temporal proximity of the investigation to the threatened litigation in determining whether the work-product doctrine applies.[46]

See Section 36.4

39 Id. at 511 (noting that '[p]roper preparation of a client's case' involves creating such documents, and that providing them to opposing counsel on 'mere demand' would be 'demoralizing' to the legal profession and disserve both clients and the 'cause of justice').

40 422 U.S. 225, 238-39 (1975).

41 Id.

42 See Fed. R. Civ. P. 26(b)(3) advisory committee's note to 1970 amendment ('[T]he weight of authority affords protection of the preparatory work of both lawyers and nonlawyers . . . .').

43 See Fed. R. Civ. P. 26(b)(3).

44 Id.

45 See *Qwest*, 450 F.3d at 1181, 1192.

46 See *Banneker Ventures, LLC v. Graham*, Civil Action No. 13-391 (RMC), 2017 WL 2124388, at *1-*2,*4-*5 (D.D.C. 16 May 2017) (finding that an internal investigation conducted 'over two years' after litigation was threatened was not conducted in anticipation of litigation and thus was not protected by the work-product doctrine).

Common interest or joint defence privilege 36.1.3

The joint defence (or 'common interest') privilege is a doctrine that preserves the attorney–client privilege and work-product doctrine, despite disclosure of otherwise protected information to third parties.[47] As explained by the Second Circuit Court of Appeals, the privilege 'serves to protect the confidentiality of communications passing from one party to the attorney for another party where a joint defense effort or strategy has been decided upon and undertaken by the parties and their respective counsel'.[48] In general, a party asserting the privilege must demonstrate that (1) the communications were made in the course of a joint defence effort, (2) the statements were designed to further the effort and (3) the privilege has not otherwise been waived.[49] If the privilege is challenged, the burden is on the defendants to demonstrate the existence of a joint defence arrangement.[50]

While a joint defence arrangement has not been held to create a direct attorney–client relationship between counsel for one party and another, some courts have found that the sharing of confidential information creates an implied attorney–client relationship among the parties to the joint defence. In *United States v. Henke*,[51] for example, the Ninth Circuit held that the joint defence privilege can, in certain circumstances, create an implied attorney–client relationship, as well as a disqualifying conflict of interest. In that case, three executives – Gupta, Desaigoudar and Henke – were charged with conspiracy, making false statements, securities fraud and insider trading.[52] All three defendants participated in joint defence meetings where they shared confidential information.[53] On the eve of trial, however, Gupta entered into a co-operation agreement and agreed to testify for the government.[54] Gupta's lawyers threatened Desaigoudar and Henke's attorneys with legal action if they revealed any confidential information obtained as part of the joint defence meetings. Desaigoudar and Henke's attorneys eventually moved to withdraw because they believed their duty of confidentiality to Gupta prevented them from effectively cross-examining him.[55] The Ninth Circuit held that the lower court erred in denying the motions to withdraw, as the joint defence privilege created 'a disqualifying conflict where information gained in confidence by an attorney [became] an issue'.[56]

47 See *United States v. Schwimmer*, 892 F.2d 237, 243-44 (2d Cir. 1989), cert. denied, 502 U.S. 810 (1991).

48 Id.

49 See, e.g., *United States v. Bay State Ambulance*, 874 F.2d 20, 28 (1st Cir. 1989); *In re Bevill, Bresler & Schulman Asset Mgmt. Corp.*, 805 F.2d 120, 126 (3d Cir. 1986); *In re Grand Jury Subpoena Duces Tecum*, 406 F. Supp. 381, 385 (S.D.N.Y. 1975).

50 See *United States v. Weissman*, 195 F.3d 96, 100 (2d Cir. 1999).

51 222 F.3d 633 (9th Cir. 2000).

52 Id. at 635.

53 Id. at 637.

54 Id.

55 Id. at 637-38.

56 Id. at 637.

To mitigate the risk that information shared in the context of a joint defence agreement may lead to disqualification at a later time, many lawyers choose to include written disclaimers in their joint defence agreements along the following lines:

> *Nothing contained [in this agreement] shall be deemed to create an attorney–client relationship between any attorney and anyone other than the client of that attorney . . . and no attorney who has entered into this Agreement shall be disqualified from examining or cross-examining any joint defense participant who testifies at any proceeding, whether under a grant of immunity or otherwise, because of such an attorney's participation in this agreement, and it is herein represented that each party to this agreement has specifically advised his or her client of this clause.*[57]

Courts have found such provisions to permit an attorney to cross-examine a witness who was a former member of a joint defence arrangement and has since become a government co-operator, and have even permitted counsel to impeach the witness using statements that would otherwise be protected as privileged under the joint defence.[58]

The recent case of *SEC v. Rashid*[59] demonstrates the importance of both confirming and recording the intention to enter into a common interest relationship. In *Rashid*, the SEC was investigating the defendant's use of corporate expenses while employed at Apollo Management LP. During the investigation, the defendant retained counsel separate from that of the company, and eventually hired a separate firm to replace the first. During a later deposition of a representative from his prior law firm, the SEC sought to inquire about discussions with company counsel. When the defendant claimed such communications were protected by common interest privilege, the SEC moved to compel the testimony, arguing that the common interest privilege is narrowly constructed and that the defendant did not meet his burden of showing that such a relationship existed. The court ordered the deposition to proceed, finding insufficient evidence of a common interest relationship. In so ruling, the court considered, among other things, (1) the lack of a written common interest agreement; (2) testimony from company counsel that they did not recall entering into a common interest relationship; (3) the

57 See *Weissman*, 195 F.3d at 100.

58 See, e.g., *United States v. Almeida*, 341 F.3d 1318, 1326 (11th Cir. 2003) (holding that statements made under the joint defence doctrine 'do not get the benefit of the attorney–client privilege in the event that the co-defendant decides to testify on behalf of the government in exchange for a reduced sentence'); *United States v. Stepney*, 246 F. Supp. 2d 1069, 1086 (N.D. Cal. 2003). (Finding that when a former codefendant testified on behalf of the government, the joint defence team could cross-examine him on statements made pursuant to a joint defence agreement that (1) specified that the agreement would not create a duty of loyalty or an attorney–client relationship; and (2) explicitly permitted the lawyer to use any material or information provided by the testifying defendant during the course of the joint defence in later cross-examining the witness.)

59 17-cv-8223, 2018 WL 6573451 (PKC) (S.D.N.Y. 13 December 2018).

defendants' lack of ability to recall specific details of the terms of the alleged agreement; and (4) that company counsel had delivered the *Upjohn* warnings at their first meeting with the defendant. The court determined that the common interest privilege cannot apply in a circumstance where there is no evidence that both parties agreed to pursue a joint legal strategy.

Further, to preserve the attorney–client privilege in the context of a joint defence arrangement, confidentiality must still be maintained against those outside the arrangement, because disclosure to a single outsider could constitute waiver of the information discussed in the outsider's presence.

Identifying the client 36.2

The 'client' in an attorney–client relationship is generally defined as the intended and immediate beneficiary of the lawyer's services, who communicates with the attorney to obtain legal advice, and interacts with the attorney to advance his or her own interests.[60] Defining the 'client' becomes more difficult in the context of corporate representation, as a company typically speaks by and through its employees, but the corporation's counsel represents not those individual agents, but rather the corporation itself.[61] As a general matter, a corporation's attorney–client privilege is controlled by the management of the organisation.[62] An employee or officer cannot assert the corporation's privilege if the corporation waives it,[63] and an employee cannot waive the corporation's privilege if the corporation asserts it.[64]

In cases where the interests of an employee are or may become adverse to that of the company during a government investigation, the Rules of Professional Conduct[65] dictate that attorneys explain clearly whom they represent.[66] Interviewing employees in the context of a government investigation inevitably creates situations in which conflict between company and employee may arise. In particular, individuals should be advised to obtain separate counsel in situations where they are (1) the target of the investigation, (2) a probable whistleblower or (3) an employee facing risk of criminal liability. In any of these circumstances, employees should not be involved in the day-to-day supervision of company counsel's own investigation, including serving in the reporting chain.

60 Greenwald & Slachetka, supra note 6, at 15-16 (citing *Wylie v. Marley Co.*, 891 F.2d 1463 (10th Cir. 1989)).

61 See, e.g., *Judson Atkinson Candies, Inc. v. Latini-Hohberger Dhimantec, Inc.*, 529 F.3d 371, 389 n.4 (7th Cir. 2008).

62 See *Commodity Futures Trading Comm'n v. Weintraub*, 471 U.S. 343, 348 (1985) (noting that 'the power to waive the corporate attorney–client privilege rests with the corporation's management').

63 See *In re Bevill*, 805 F.2d at 124-25; *In re Hechinger Inv. Co.*, 285 B.R. 601, 606 (D. Del. 2002) (finding that former officers and employees could not assert the corporation's privilege).

64 See *In re Grand Jury Proceedings*, 219 F.3d 175, 184 (2d Cir. 2000).

65 American Bar Association, Center for Professional Responsibility, Model Rules of Professional Conduct (2016), http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html.

66 ABA Model Rule of Professional Conduct 1.13(f).

Company counsel may encounter circumstances where an employee seeks to assert the attorney–client privilege to prevent the disclosure of information uncovered by counsel during investigative interviews by arguing that company counsel represents the employee as an individual. The Third Circuit in *In re Bevill Bresler & Schulman Asset Management Corp*, developed a five-part test (the *Bevill* test) to examine the merits of such an assertion by an individual employee against company counsel.[67] Under this test, employees must show that (1) they approached corporate counsel for the purpose of seeking legal advice, (2) they made it clear that they were seeking advice in their individual capacity, (3) counsel sought to communicate with the employee in this individual capacity, mindful of the conflicts with its representation of the company, (4) the communications were confidential and (5) the communications did not concern the employee's official duties or the general affairs of the company.[68] The *Bevill* test has been recognised by other jurisdictions as a means of assessing whether a company employee may assert attorney–client privilege in an individual capacity arising out of communications with corporate counsel.[69]

See Chapter 14 on employee rights

In *United States v. Blumberg*,[70] for example, the District of New Jersey applied the *Bevill* test where an individual employee sought to claim personal privilege protection for communications with the company's lawyer. In assessing the fifth factor of the test, the court considered the individual employee's claim that he had discussed with company counsel his 'potential for criminal exposure' and the fact that he was just a 'fact witness'.[71] The court ultimately concluded that this exchange did not create an individual attorney–client relationship, and that the company still owned the privilege covering the employee's communications, and thus could waive it (presumably over his objection).[72]

To mitigate the risks created by potentially divergent interests between the company and individual employees, counsel should be clear in their engagement letter about not only whom they represent, but also whom they do not. Further, mindful of the considerations outlined by the *Bevill* court, company counsel should take care during interviews with individual employees to limit their discussions to matters within the scope of the employee's official duties, rather than matters that may implicate the employee's personal interests. Finally, in the event that discussions with an individual employee diverge to matters implicating legal advice in the employee's individual capacity, counsel should reiterate

67 805 F.2d 120, 123, 125 (3rd Cir. 1986).

68 Id.

69 See, e.g., *United States v. Int'l Bhd. of Teamsters, Chauffeurs, Warehousemen & Helpers of Am.*, AFL-CIO, 119 F.3d 210, 215 (2d Cir. 1997); *United States v. Graf*, 610 F.3d 1148, 1160-61 (9th Cir. 2010) (adopting the Bevill test and listing other jurisdictions who have adopted the test as well).

70 2017 U.S. Dist. LEXIS 47298 (D.N.J. 27 Mar. 2017).

71 Id. at *14.

72 Id. at *14-15.

to the employee that they have been retained to represent the company and the company's interests, and potentially advise the employee to retain separate counsel with respect to these other matters.

Maintaining privilege 36.3

Employee interviews 36.3.1

It is generally best if counsel conducts the employee interviews in the context of a government investigation, to ensure that what is said during the interview is covered by the attorney–client privilege, and that notes or memoranda documenting the interview are similarly privileged.[73] Recordings of interviews may, however, be considered purely factual communications that – as verbatim transcriptions – may not be subject to the attorney work-product doctrine.[74] Accordingly, it is general practice to have the attorney interviewer (or, more likely, another attorney in the room) take written notes of the interviews that include his or her thoughts and mental impressions. And because opinion work-product receives greater protection than fact work-product, it is more likely that written notes including an attorney's thoughts and impressions will be protected.[75]

While it is often most advantageous to have counsel conduct the witness interviews in an investigation, a court may still find that interviews conducted by non-lawyers maintain attorney–client privilege if they are acting as agents for lawyers. For example, in *In re Kellogg Brown & Root Inc* (*KBR*),[76] the DC Circuit court held that the work of an engineering and construction firm involved in an the internal investigation was afforded work-product protection where the investigation was conducted 'under the auspices of KBR's in-house legal department, acting in its legal capacity'.[77] The court held that '[s]o long as obtaining or providing legal advice was one of the significant purposes of the internal investigation,

73 *Upjohn*, 449 U.S. at 394-99 (explaining that attorney–client privilege protects attorney notes taken during interviews with employees during internal investigations); see also *In re Gen. Motors Ignition Switch Litig.*, 80 F. Supp. 3d 521, 527-28 (S.D.N.Y. 2015) (finding that documents related to the internal investigation were protected from discovery because (1) the investigation was conducted at the direction of counsel; (2) those interviewed were told that the purpose of the interview was to facilitate the rendering of legal advice; (3) they were told that that the content of the discussions should remain confidential; and (4) the communications underlying the published report were not shared with third parties).

74 See Fed. R. Crim. P. 26.2(a), (f)(2); see also *United States v. Nobles,* 422 U.S. 225, 230-32 (1975).

75 It is critical for counsel to establish the expectation of confidentiality and attorney–client privilege protection at the outset of each interview, as interview memoranda merely labelled as privileged and confidential will not 'retroactively render the earlier, otherwise-unprivileged discussions subject to the attorney–client privilege.' See E*rickson v. Hocking Technical College*, Case No. 2:17-cv-360, 2018 U.S. Dist. LEXIS 50075, at *6, *8 (S.D. Ohio 27 March 2018).

76 756 F.3d 754 (D.C. Cir. 2014).

77 *KBR*, 756 F.3d at 757 (citing *Upjohn*, 449 U.S. 383).

the attorney–client privilege applies'.[78] The court's decision in *KBR* underscores the importance of making it clear that witness interviews conducted in the context of an internal investigation are for the purpose of rendering legal advice.[79]

Consistent with these principles, at the outset of any employee interview, counsel should give the employee an *Upjohn* warning, which makes clear that the communications between company counsel and the employees are confidential and protected as attorney–client privileged, and specifies that the privilege belongs to the company, and the company may choose to waive that privilege in the future. If clearly given, an *Upjohn* warning sets the boundaries of the interview and removes any doubt about whether counsel represents the employee.

In *KBR*, the DC Circuit noted that there are no 'magic words' that must be used to deliver a proper *Upjohn* warning.[80] Nevertheless, in practice, *Upjohn* warnings typically include some variation of the following components:

- *The lawyer represents the company only and not the witness personally.*
- *The lawyer is collecting facts for the purpose of providing legal advice to the company.*
- *The communication is protected by attorney–client privilege, which belongs exclusively to the company, not the witness.*
- *The company may choose to waive the privilege and disclose the communication to a third party, including the government.*
- *The communication must be kept confidential, meaning that it cannot be disclosed to any third party other than the witness's counsel.*[81]

Once the *Upjohn* warning is given, and before any substantive interview commences, counsel should confirm that the witness understands the warning, answer any questions the witness has about it and establish that the witness is agreeable to being interviewed under these terms. As an additional precaution, counsel should remind the witness at the conclusion of the interview not to discuss the substance of the interview with anyone else, except to the extent that the witness wishes to convey additional information or to ask follow-up questions of counsel.

Once a witness interview is complete, memorialising the content of the interview is essential to the investigation. The summary should state expressly that it does not constitute a verbatim transcription of the interview and that the

78 Id. at 758-59.

79 In contrast, in *Wultz v. Bank of China*, the Southern District of New York granted a motion to compel documents collected by non-lawyers in the context of an internal investigation, where the party invoking the privilege failed to demonstrate that the documents were collected at the direction of an attorney to assist the attorney in providing legal advice. 304 F.R.D. 384, 395-97 (S.D.N.Y. 2015). The court also found that the work-product doctrine would not protect the documents from disclosure because the bank had failed to show that the documents would not have been created in 'essentially similar form irrespective of the litigation.' Id. at 395.

80 *KBR*, 756 F.3d at 758.

81 See, e.g., ABA, White Collar Working Group, *Upjohn Warnings: Recommended Best Practices When Corporate Counsel Interacts With Corporate Employees* (17 July 2009).

summary contains the thoughts, mental impressions and legal conclusions of counsel. The summary should also confirm the delivery of the *Upjohn* warning, indicating the employee's understanding of the warning and willingness to proceed with the interview.

The importance of recording the provision of the *Upjohn* warning is underscored by the case of *United States v. Ruehle*.[82] In *Ruehle*, outside counsel conducted an interview of an employee, William J Ruehle, during an internal investigation. During the interview, Ruehle made statements that he later sought to suppress from his criminal trial. He argued that the statements were privileged because outside counsel had previously represented him in his individual capacity in a shareholder lawsuit, and counsel had not otherwise advised him that his statements during the internal investigation could be disclosed to third parties. The court found there to be inadequate evidence that Ruehle had been given *Upjohn* warnings, finding it persuasive that there was no reference to their delivery in counsel's interview memoranda. While the court's decision was later reversed on other grounds, this case illustrates the importance of maintaining a record of the delivery of *Upjohn* warnings.

See Chapters 8 on witness interviews and 14 on employee rights

Issues may also arise when interviewing current employees in the context of an internal investigation, to the extent that the investigation is prompted by a government inquiry when there is extensive coordination with a government regulator. In *United States v. Connolly*,[83] a bank engaged outside counsel to conduct an investigation into the bank's LIBOR practices that was prompted by a letter from the Commodity Futures Trading Commission (CFTC) requesting that the bank 'cooperate fully' by 'voluntarily engaging' outside counsel to conduct a review. During the investigation, outside counsel 'coordinated extensively' with both the CFTC and the Department of Justice (DOJ), and the government agencies gave substantial direction to the lawyers as to which employees should be interviewed and how to approach the interviews. After a bank employee, Connolly, was later indicted and convicted for conspiracy and wire fraud for his conduct in connection with the manipulation of LIBOR, he moved to vacate his conviction on the theory that his prosecution was predicated on, and fatally tainted by, statements that he gave in interviews conducted by outside counsel during the investigation. He argued that counsel was effectively deputised by the government in conducting the interviews, and as a result his statements should be deemed involuntary and rendered inadmissible under *Garrity v. New Jersey*,[84] since he made the statements under the threat of termination of employment in violation of his Fifth Amendment rights. Chief Judge Colleen McMahon of the Southern District of New York found that outside counsel here was '*de facto* that Government for *Garrity* purposes' and noted that she was 'deeply troubled by this issue', which had 'profound implications' for how government investigations are conducted. And while the Court ultimately declined to overturn the employee's conviction,

82 583 F.3d 600 (9th Cir. 2009).

83 No. 16-Cr-00370, 2019 WL 2120523 (S.D.N.Y. 2 May 2019).

84 385 U.S. 493 (1967).

holding that the government did not 'use' his compelled statements in indicting or prosecuting him, the Court's comments and admonition will undoubtedly have a significant impact on the level of coordination with government agencies in investigations going forward.

See Chapter 10 on co-operating with authorities

36.3.2 Former employees

Interviews with former corporate employees about matters within the scope of their prior employment may also be protected by the attorney–client privilege.[85] Indeed, while courts of different jurisdictions are split as to whether attorney–client privilege should extend to discussions with former employees as a general matter,[86] most courts agree that narrowly tailored discussions related to the period of the individual's former employment should remain privileged.[87] As such, counsel conducting an investigation should carefully focus the interview with a former employee on matters that occurred during the former employee's tenure, as some district courts have held that interviews with a former employee on subjects that occurred after the employment had ended are not privileged.[88]

In determining whether a former employee is likely to be co-operative or to maintain the confidentiality of the interview, counsel should consider (1) the circumstances of the employee's departure and (2) whether the employee will be contractually obliged to maintain the confidentiality of the interview, through a severance agreement, for example.

36.3.3 Non-legal advice

At the outset of an internal investigation, the corporation should document that the investigation is being conducted for the purpose of obtaining legal advice and at the direction of counsel. If such intention is not documented, and it appears

85 *Upjohn*, 449 U.S. at 403 (Burger, C.J., concurring) (finding a former employee's communication is privileged when the employee 'speaks at the direction of the management with an attorney regarding conduct or proposed conduct within the scope of employment').

86 Compare *In re Coordinated Pretrial Proceedings in Petroleum Prod. Antitrust Litig.*, 658 F.2d 1355, 1361 n. 7 (9th Cir. 1981) (finding that the *Upjohn* rationale extended the attorney–client privilege to former employees because 'former employees . . . may possess the relevant information needed by corporate counsel to advise the client with respect to actual or potential difficulties.'), with *Clark Equip. Co. v. Lift Parts Mfg Co.*, No. 82 C 4585, 1985 WL 2917, at *5 (N.D. Ill. 1 Oct. 1985) (declining to apply privilege protection to communications with former employees, noting that '[i]t is virtually impossible to distinguish the position of a former employee from any other third party who might have pertinent information about one or more corporate parties to a lawsuit').

87 See, e.g., *United States ex rel. Hunt v. Merck-Medco Managed Care, LLC*, 340 F. Supp. 2d 554, 558 (E.D. Pa. 2004) ('the line to be drawn is not difficult: if the communication sought to be elicited relates to [the former employee's] conduct or knowledge *during* her employment . . . , or if it concerns conversations with corporate counsel that occurred *during* her employment, the communication is privileged; if not, the attorney–client privilege does not apply') (emphasis in original).

88 See, e.g., *United States ex rel. Hunt v. Merck-Medco Managed Care, LLC*, 340 F. Supp. 2d 554, 558 (E.D. Pa. 2004); *Peralta v. Cendant Corp.*, 190 F.R.D. 38, 41 (D. Conn. 1999). Interviews about such topics may, however, be covered by work-product protection.

instead that employee interviews are being conducted in the context of a non-legal investigation, such communications may not be effectively cloaked in the attorney–client privilege. In *Koumoulis v. Independent Financial Marketing Group Inc*,[89] for example, plaintiffs were former and current employees of a company in the business of providing investment products to financial institutions.[90] The Eastern District of New York found that reports documenting internal discrimination complaints and the subsequent investigation by the company's human resources managers were not protected as attorney–client privileged because 'their predominant purpose was to provide human resources and thus business advice, not legal advice.'[91]

In light of *Koumoulis*, counsel must be ever mindful of stating explicitly at the outset of an investigation that its communications are outside the course of the day-to-day operation of the client's business and are explicitly aimed at assisting the delivery of legal advice. To the extent that litigation is reasonably foreseeable, it should be noted in all memoranda generated in the context of the investigation. Further, counsel should confirm with individual employees that when they are seeking legal advice – rather than business advice – the employees should be similarly explicit in their communications, labelling them as 'attorney–client privileged'. More important than any label or transcription, however, is that the context of such documents must reflect the solicitation and receipt of legal, rather than business, advice.[92]

Waiving privilege 36.4

Even if all the prerequisites for establishing attorney–client privilege are met, whenever a client discloses confidential communications to third parties, including government agencies, the disclosure may constitute a waiver of the privilege as to both the communication that has been disclosed and other communications relating to the same subject matter. Federal Rule of Evidence 502(a) governs disclosures made to a federal officer or agency and also the scope of waiver in such disclosures.[93] The rule explicitly states that disclosures of attorney–client or work-product protection to the federal government creates a waiver that extends to other undisclosed communication or information in a federal or state proceeding

89 295 F.R.D. 28 (E.D.N.Y. 1 November 2013), aff'd in part, 29 F. Supp. 3d 142 (E.D.N.Y. 21 January 2014).

90 Id. at 33.

91 Id. at 46. See also *Welland v. Trainer*, No. 00 Civ. 0738(JSM), 2001 WL 1154666, at *2 (S.D.N.Y. 1 October 2001) (finding certain communications between the investigator, who conducted the internal investigation, and in-house and outside counsel are protected by attorney–client privilege because the investigator received legal advice from counsel under circumstances in which the employee under investigation was an executive and litigation was expected if the employee were terminated).

92 *Koumoulis*, 29 F. Supp. 3d at 147 (finding that legal memoranda must contain more than 'a stray sentence or comment within an email chain referenc[ing] litigation strategy or advice').

93 Fed. R. Evid. 502(a).

if: (1) the waiver is intentional, (2) the disclosed and undisclosed communications or information concern the same subject matter and (3) they ought in fairness to be considered together.[94]

While the 'fairness' requirement of Rule 502(a) creates some uncertainty as to when subject-matter waiver might occur, in practice, courts typically look to the reason for the initial disclosure when determining the scope of a waiver. If a court determines that a party selectively disclosed privileged information to gain a strategic advantage to the government's detriment, it is more likely to find a full subject-matter waiver.[95] But, if the disclosure occurred outside the context of litigation, or if the disclosure was not intended for – or did not actually result in – a strategic advantage to the disclosing party, the court is likely to find a limited waiver.[96] In the case of *United States v. Treacy,*[97] for example, Judge Rakoff of the Southern District of New York quashed a defendant's subpoena for a law firm's interview memoranda that had not previously been provided to the government, rejecting the theory that furnishing some interview memoranda to the government waived privilege to others covering the same subject matter.[98] The Court relied on the advisory committee notes in Rule 502(a) in support of its 'fairness' assessment, finding that subject-matter waiver should be reserved for the narrow circumstances where a party seeks to disadvantage their adversary through a selective or misleading disclosure.[99] Further, if a party chooses to disclose attorney work-product to the government – in the form of White Papers, presentations or other memoranda – with the purpose of dissuading the government from bringing suit, one court has recently held that such a disclosure will waive any privilege with respect to those materials, which may subsequently be discoverable by third parties.[100]

---

94 Id.

95 See, e.g., *In re Teleglobe Commc'ns Corp.,* 493 F.3d 345, 361 (3d Cir. 2007). ('When one party takes advantage of another by selectively disclosing otherwise privileged communications, courts broaden the waiver as necessary to eliminate the advantage.')

96 See, e.g., *In re Keeper of the Records,* 348 F.3d 16, 24 (1st Cir. 2003) (holding that 'the extrajudicial disclosure of attorney–client communications, not thereafter used by the client to gain adversarial advantage in judicial proceedings, cannot work an implied waiver of all confidential communications on the same subject matter'); *Swift Spindrift, Ltd. v. Alvada Ins. Inc.*, No. 09 Civ. 9342 (AJN)(FM), 2013 WL 3815970, at *5 (S.D.N.Y. 24 July 2013) (finding that the intentional disclosure of two privileged emails did not result in a broader waiver of the attorney–client privilege because (1) the emails were actually unfavourable to the disclosing party's position; and (2) therefore could not be used to the other parties' disadvantage).

97 No. S2 08 CR 366 (JSR), 2009 WL 812033 (S.D.N.Y. 24 Mar. 2009).

98 Id. at *1-2.

99 Id.

100 See *Alaska Electrical Pension Fund v. Bank of America Corp.*, 2017 WL 280816. at *2-3 (S.D.N.Y. 20 January 2017); See also SEC Division of Enforcement, *Enforcement Manual*, Office of the Chief Counsel. §3.2.3.2 (28 October 2016) (specifying that White Papers, excluding Wells notices, submitted to the SEC may be discoverable by third parties in accordance with applicable law).

Co-operation credit and waiver 36.4.1

Corporations subject to criminal or regulatory investigations have long faced the question of whether and when to turn over privileged material to the government. Waiving privilege has historically resulted in increased co-operation 'credit' from the DOJ[101] and the Securities and Exchange Commission (SEC).[102] However, changes to DOJ guidelines now forbid the government from requesting that companies waive attorney–client privilege, and preclude consideration of whether the corporation waived privilege in assessing co-operation credit.

Indeed, in response to pressure from the private sector and the legislative and judicial branches, on 12 December 2006, the then Deputy Attorney General Paul J McNulty issued a memorandum containing new corporate charging guidelines for federal prosecutors through a revision to the Principles of Federal Prosecution of Business Organizations.[103] The McNulty Memorandum required that, before requesting a waiver of attorney–client or work-product privileged information from a corporation under investigation, prosecutors must establish a 'legitimate need' for privileged communications and seek approval of the US Attorney, who must obtain written approval of the Deputy Attorney General.[104]

In 2008, the DOJ replaced these guidelines in a memorandum authored by then Deputy Attorney General Mark R Filip.[105] The Filip Memorandum further adjusted what factors the government should consider in determining whether a corporation deserves 'co-operation credit': where co-operation credit had previously turned on factors including waiver of attorney–client privilege or work-product protections, it will now focus on disclosure of relevant facts.[106] In other words, a company could receive the same co-operation credit if it disclosed facts contained in non-privileged materials as it would if it disclosed facts contained in privileged materials, so long as the company discloses all relevant facts known to it.

101 See, e.g., Memorandum from Larry D Thompson, Deputy Att'y Gen., U.S. Dep't of Justice, to Heads of Department Components and United States Attorneys, regarding Principles of Federal Prosecution of Business Organizations (20 January 2003) (Thompson Memorandum); see also Memorandum from Paul McNulty, Deputy Att'y Gen., U.S. Dep't of Justice, to Heads of Department Components and United States Attorneys, regarding Principles of Federal Prosecution of Business Organizations (12 December 2006) (McNulty Memorandum).

102 See, e.g., Sec. & Exch. Comm'n, SEC Rel. No. 34-44969, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions (the Seaboard Report) (23 October 2001) (explaining that a company that disclosed internal investigation interviews without asserting privilege had fully co-operated).

103 McNulty Memorandum, supra note 95.

104 Id. at 8-9.

105 Memorandum from Mark R Filip, Deputy Att'y Gen., U.S. Dep't of Justice, to Heads of Department Components and United States Attorneys, regarding Principles of Federal Prosecution of Business Organizations (28 August 2008) (Filip Memorandum).

106 Id.

In September 2015, the DOJ issued a memorandum authored by then Deputy Attorney General Sally Quillian Yates entitled 'Individual Accountability for Corporate Wrongdoing'.[107] The Yates Memorandum set forth policies intended to guide the DOJ in holding individual defendants civilly and criminally liable for corporate misconduct.[108] Significantly, the Yates Memorandum now requires a company to disclose 'all relevant facts relating to the individuals responsible for the misconduct' for the company 'to be eligible for any cooperation credit'.[109] While Yates has publicly remarked that these new policies are not intended to undermine the Filip Memorandum's guidance regarding the waiver of attorney–client privilege,[110] the mandate to disclose 'all relevant facts' creates some uncertainty as to whether, at least practically speaking, such a waiver may now be required once again. In describing the impact of the Yates Memorandum on companies seeking co-operation credit, Yates explained the DOJ's view that 'facts are not [privileged]', and therefore a company must 'produce all relevant facts – including the facts learned through . . . interviews [with company employees] – unless identical information has already been provided.'[111]

In November 2017, the DOJ adopted the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy, which provided guidance regarding the credit that the DOJ might provide to companies who self-report FCPA violations. The policy authorises certain benefits – including a presumption that self-reporting companies will not be criminally charged – for companies that meet the DOJ's rigorous requirements of disclosure, co-operation and remediation, including disgorgement of ill-gotten gains.[112] In March 2018, the DOJ announced an expansion of the FCPA Corporate Enforcement Policy, noting that it may be employed as non-binding guidance in criminal cases beyond those arising under the FCPA. This announcement underscores the DOJ's encouragement of self-reporting and co-operation by companies in a wide range of criminal cases.

On 29 November 2018, Deputy Attorney General Rod J Rosenstein delivered remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act[113] that reaffirmed the central tenets of the

107 Memorandum from Sally Quillian Yates, Deputy Att'y Gen., U.S. Dep't of Justice, to Heads of Department Components and United States Attorneys, regarding Individual Accountability for Corporate Wrongdoing (9 September 2015) (Yates Memorandum).

108 Id. at 1.

109 Id. at 2.

110 Remarks of Deputy Att'y Gen. Sally Quillian Yates delivered at American Banking Association and American Bar Association Money Laundering Enforcement Conference (16 November 2015), available at https://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-american-banking-0 ('[T]here is nothing in the new policy that requires companies to waive attorney–client privilege or in any way rolls back the protections that were built into the prior factors.').

111 Id.

112 Corporate Enforcement Policy, U.S. Dep't of Justice, Justice Manual § 9-47.120 (2017), available at https://www.justice.gov/criminal-fraud/corporate-enforcement-policy.

113 See Deputy Attorney General Rod J Rosenstein Delivers Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act, Office of

Yates Memorandum, but also announced a revised policy that provides federal prosecutors with greater discretion concerning whether to pursue individuals, based on varying standards between civil and criminal investigations. In particular, Rosenstein stated that companies are no longer expected to 'admit the civil liability of every individual employee' to qualify for co-operation credit. Instead, companies should focus on identifying individuals who were 'substantially involved in or responsible for the misconduct', including members of senior management or the board of directors. While Rosenstein's comments have been considered as a reversion to pre-Yates priorities, where the 'primary goal' in civil cases is to recover money, recent court decisions have demonstrated a continued focus on the concepts of individual accountability articulated by Yates.[114]

In light of this recent guidance, corporate counsel must be mindful about entering into joint defence agreements that might limit their ability to share with the government the underlying facts learned during the investigation, especially if the company is facing exposure to a potentially devastating criminal charge if it does not receive credit for co-operating with the government. In addition, the Yates Memorandum underscores the importance of issuing comprehensive *Upjohn* warnings when interviewing company employees, as a mandate to disclose 'all relevant facts' may involve the revelation to the government of facts disclosed by (potentially culpable) employees in the context of investigative interviews.

Inadvertent disclosure of privileged material 36.4.2

Particularly in cases where large numbers of documents are produced, it is not uncommon that a party might inadvertently disclose privileged communications. Federal Rule of Evidence 502(b) governs the court's treatment of attorney–client privileged and work-product material that has been inadvertently disclosed. The rule provides that, when making a disclosure in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if: '(1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error.'[115] According to Rule 502(b)'s advisory committee explanatory notes, courts are to consider several factors in determining whether the privilege holder took steps to promptly rectify the error, including (1) the reasonableness of precautions taken, (2) the time taken to rectify the error, (3) the scope of discovery, (4) the number of documents reviewed and the time constraints for production, (5) the extent of disclosure and (6) 'the

Public Affairs, U.S. Dep't of Justice (29 November 2018) https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

114 See *United States ex rel. Doe v. Heart Solutions PC et al.*, 923 F.3d 308, 314-15 (3d Cir. 2019) (sustaining summary judgment against an individual defendant even though she had no financial stake in the corporation profiting from the fraud, citing the Yates memorandum as endorsing enforcement under the false claims act against individuals 'at all levels' of the corporate structure.)

115 Fed. R. Evid. 502(b).

overriding issue of fairness'.[116] The explanatory notes also suggest that a party can help demonstrate that its steps were reasonable by employing 'advanced analytical software applications and linguistic tools' in screening for privilege.[117]

Federal Rule of Civil Procedure 26(b)(5)(B) provides additional guidance on how clawback provisions may intersect with a claim of inadvertent disclosure. Under this rule, if information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, 'the party making the claim may notify any party that received the information of the claim and the basis for it'.[118] After being notified, a party:

> *must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim*.[119]

While the same clawback procedure is not explicitly contemplated in the criminal context, parties making disclosures in federal proceedings or to a federal office or agency may choose to enter into a voluntary clawback arrangement under Rule 502(e), including an explicit agreement that inadvertent disclosure will not constitute a waiver.[120] Such agreements are generally binding only on the parties to the agreement.[121] A carefully drawn clawback agreement can be to the benefit of everyone in the context of a government investigation: the agency will benefit from receiving discovery more expeditiously, and the producing party will benefit from minimising the risk and added review costs in the absence of such an agreement.[122] Even where counsel takes reasonable steps to prevent the disclosure of privileged material, the complexity of government investigations creates a real risk that such materials may still be inadvertently produced. To further mitigate this risk, document production letters should include unequivocal language, preserving the client's ability to claw back and recover inadvertently disclosed documents.

36.5 Selective waiver

The attempt to disclose privileged material to the government in the context of an investigation, while still claiming privilege and confidentiality over that same material as to other third parties, is called 'selective waiver'. Generally, courts have refused to sanction selective waiver, finding that the disclosure of privileged

116 Fed. R. Evid. 502 advisory committee's note.

117 Id.

118 Fed. R. Civ. P. 26(b)(5)(B).

119 Id.

120 Fed. R. Evid. 502(e).

121 Id.

122 In the context of an investigation that is already public, a party may choose to request a court order limiting the scope of waiver and/or setting forth a clawback procedure to govern its production. See Fed. R. Evid. 502(d).

material to the government destroys the confidentiality necessary to maintain a claim of privilege in the first place, and therefore waives the privilege with respect to other third parties as well.[123]

The leading case applying the selective-waiver analysis is *Diversified Industries Inc v. Meredith*.[124] In *Diversified Industries*, a corporation retained external counsel to conduct an internal investigation into allegations of bribery.[125] The internal report prepared by external counsel was then produced to the SEC.[126] The Eighth Circuit held that this disclosure constituted only a 'limited waiver' that did not preclude the corporation from subsequently withholding the report from private litigants on the grounds of attorney–client privilege.[127] The court reasoned that a contrary ruling may undermine corporate incentives to initiate internal investigations conducted by counsel.[128]

But while *Diversified Industries* is still good law, the concept of selective waiver is disfavoured by most federal circuit courts,[129] which routinely hold that selective disclosure of a document to the government constitutes complete waiver of the privilege. As the DC Circuit reasoned, the privilege was not designed to allow a client 'to pick and choose among his opponents, waiving the privilege for some and resurrecting the claim of confidentiality to obstruct others'.[130]

The Second Circuit confronted the issue of selective waiver in *In re Steinhardt Partners LP*.[131] While expressing reluctance to embrace selective waiver, the *Steinhardt* decision refused to foreclose the possibility that selective waiver may be found in some cases, at least where the disclosing party and the government share a common interest or the disclosing party has entered into an explicit agreement with the government to maintain the confidentiality of the disclosed materials.[132] As a result, in the Second Circuit, a case-by-case analysis of the facts is necessary to determine whether selective waiver may apply.[133]

The recent case of *SEC v. Herrera*[134] illustrates the risks of selective waiver inherent in making a proffer to the government. In *Herrera*, external counsel conducted an internal investigation into certain apparent accounting errors in the company's books and records. During a subsequent SEC investigation, counsel

123 See, e.g., *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289 (6th Cir. 2002); *United States v. Mass. Inst. of Tech.*, 129 F.3d 681 (1st Cir. 1997); *Westinghouse Elec. Corp. v. Republic of the Philippines*, 951 F.2d 1414 (3d Cir. 1991); *In re Martin Marietta Corp.*, 856 F.2d 619 (4th Cir. 1988); *Permian Corp. v. United States*, 665 F.2d 1214 (D.C. Cir. 1981).

124 572 F.2d 596 (8th Cir. 1977) (en banc).

125 Id. at 607.

126 Id. at 600.

127 Id. at 611.

128 Id.

129 See, e.g., *In re Pac. Pictures Corp.*, 679 F.3d 1121 (9th Cir. 2012) (asserting that the doctrine has been 'rejected by every other circuit to consider the issue since' Diversified Industries).

130 *Permian Corp.*, 665 F.2d at 1219-20.

131 9 F.3d 230 (2d Cir. 1993).

132 Id. at 236.

133 Id.

134 324 F.R.D. 258 (S.D. Fl. 2017).

was forthcoming to the SEC about documents that it uncovered over the course of its investigation, provided the SEC with a PowerPoint presentation that set forth its investigative steps and factual findings, and provided 'oral downloads' to the SEC of each of the 12 witness interviews it conducted. When former officers of the company were later sued in an SEC action, the defendants subpoenaed the records from the internal investigation during discovery, requesting (among other things) the law firm's written notes and memoranda from the witness interviews that had been described to the SEC and referenced in the PowerPoint presentation. The court rejected the law firm's argument that work-product protection still applied to the interview memoranda, finding that counsel's oral disclosures of their contents was the 'functional equivalent' of giving the SEC the memoranda themselves, removing any protection from them. The court acknowledged that the outcome may have been different had the external law firm only provided 'vague references' to the contents of the memo, or 'conclusions or general impressions' that were free of detail.[135] The court, reflecting the fact-specific nature of these determinations, however, did not find a broader subject matter waiver to the other findings referenced in counsel's presentation.

In *In re Grand Jury Investigation*,[136] in the context of the United States Special Counsel's Office (SCO) investigation of foreign interference in the 2016 presidential election, the SCO uncovered evidence that Paul Manafort (President Donald Trump's former campaign manager), his lobbying company and its employees made false statements in two letters submitted to the Foreign Agent Registration Act Registration Unit. In the first letter, counsel made factual representations that her clients did not have any agreements to provide services to a foreign entity. In the follow-up letter, counsel represented that one client could 'recall interacting' with consultants for a foreign entity, but did not recall meeting with or conducting outreach or facilitating any phone calls. The grand jury subsequently subpoenaed the attorney to testify about the communications underlying the factual representations in the letters. The attorney refused to answer the questions, citing attorney–client privilege and work-product protection. The court found that counsel had waived, through voluntary disclosure, all attorney–client privilege as to the contents of the letters, which 'made specific factual representations' that are 'unlikely to have originated from sources other than the Targets, and, in large part, were attributed to the Targets' recollections',[137] and extended the waiver to all communications on that same subject matter. The court also found that the crime-fraud exception provided an independent basis for waiver of privilege with respect to several of the questions posed to counsel in the grand jury.[138]

Some courts have suggested that production pursuant to a valid confidentiality agreement entered into with the government prior to the disclosure of attorney–client privileged or work-product information effectively preserves the

135 Id. at 264.

136 No. 17-2336, 2017 WL 4898143 (D. D.C., 2 October 2017).

137 Id. at *11.

138 Id. at *15.

privilege and does not amount to a waiver as to third parties.[139] Consequently, if the company does intend to disclose privileged material to the government, it should first attempt to obtain such an agreement from the government that it will keep the information confidential (a McKesson letter).[140] But even though future plaintiffs would not be parties to such an agreement, some courts have still found that the production of privileged materials pursuant to confidentiality agreements with the government nonetheless constitutes a waiver.[141] In light of federal courts' reluctance to find selective waiver, when a company voluntarily discloses documents or communications to government agencies, it must do so with the understanding that the documents and communications may lose the protection of the privilege and be subject to discovery by other parties, including private litigants.

Safe harbours

Banks, in particular, often face pressure to share privileged materials with the government, both in the context of enforcement actions aimed at suspected wrongdoing and during routine regulatory oversight. But as a statutory matter, sharing privileged materials with bank supervisors results in a waiver of privilege only with respect to those supervisors; it does not waive applicable privileges with respect to third parties. Under Section 1828(x) of the Regulations Governing Insured Depository Institutions, the submission of information to 'the Bureau of Consumer Financial Protection, any [f]ederal banking agency, [s]tate bank supervisor, or foreign banking authority for any purpose in the course of any supervisory or regulatory process' shall not be construed as waiving privilege 'as to any person or entity other than such agency, supervisor, or authority'.[142] This approach provides one of the few examples of federal statutes that explicitly allow for the idea of selective waiver.[143]

Disclosure to third parties 36.6

Generally, the attorney–client privilege is waived if the holder of the privilege voluntarily discloses or consents to the disclosure of any significant part of the communication to a third party or stranger to the attorney–client relationship.[144] A third-party agent may have communications with an attorney that remain covered by the attorney–client privilege if the agent's role is limited to helping a lawyer

139 See, e.g., *Dellwood Farms, Inc. v. Cargill, Inc.*, 128 F.3d 1122, 1127 (7th Cir. 1997); *In re Subpoenas Duces Tecum*, 738 F.2d 1367, 1375 (D.C. Cir. 1984); *In re Natural Gas Commodity Litig.*, No. 03 Civ. 6186 (VM) (AJP), 2005 U.S. Dist. Lexis 11950, at *39 (S.D.N.Y. 21 June 2005).

140 See David N. Powers & Sara E. Kropf, Disclosure of Internal Investigation Reports: A Legislative Solution to the McKesson Letter Dilemma, 32 Sec. Reg. L.J. 340, 341 (2004).

141 See, e.g., *In re Columbia/HCA Healthcare Corp.*, 293 F.3d at 302-04; *Westinghouse Elec. Corp.*, 951 F.2d at 1424-27, 1431.

142 12 U.S.C. § 1828(x).

143 Section 1828(x)'s companion statute, 12 U.S.C. § 1785(j), applies the same rule to credit unions.

144 See *In re Grand Jury Proceedings*, No. M-11-189 (LAP), 2001 WL 1167497, at *7 (S.D.N.Y. 3 October 2001).

give effective advice to the client.[145] Whether disclosure to external consultants will constitute a waiver will depend on the surrounding facts and circumstances, including the purpose for the disclosure and the involvement of counsel with that third party.[146]

United States v. Kovel is the seminal case concerning the bounds of attorney–client privilege with respect to third-party consultants.[147] In *Kovel*, a law firm employed an accountant who was held in criminal contempt for refusing to testify about his conversations with the law firm's client under a claim of privilege.[148] In considering whether the accountant had a basis to assert attorney–client privilege, the Second Circuit recognised that there are situations 'where the lawyer needs outside help', and found that when the accountant assists in the 'effective consultation between the client and the lawyer which the privilege is designed to permit', the privilege should protect the communications.[149] The *Kovel* court analogised the accountant's role to that of an interpreter, which is sometimes necessary for the attorney effectively to communicate with his or her client.[150] The *Kovel* doctrine has been recognised by many courts as protecting attorney–client privilege in circumstances where a third party has specialised knowledge or skills that assist the attorney in rendering legal advice.[151] To preserve attorney–client privilege in such circumstances, the consultant is typically appointed directly by counsel and works under counsel's supervision. The mere hiring of the consultant through counsel, however, will not automatically cloak the third-party communications in

145 See *United States v. Kovel,* 296 F.2d 918, 922 (2d Cir. 1961).

146 See, e.g., *Fed. Trade Comm'n v. GlaxoSmithKline*, 294 F.3d 141, 148 (D.C. Cir. 2002) (finding 'no reason to distinguish between a person on the corporation's payroll and a consultant hired by the corporation if each acts for the corporation and possesses the information needed by attorneys in rendering legal advice'); *NXIVM Corp. v. O'Hara*, 241 F.R.D. 109, 131-32 (N.D.N.Y. 2007) (finding that when attorney acted solely as coordinator of media relations, communications between attorney and client were not protected). See generally Michele DeStefano Beardslee, The Corporate Attorney–Client Privilege: Third-Rate Doctrine for Third-Party Consultants, 62 SMU L. Rev. 727, 744-55 (2009) (outlining the doctrine of attorney–client privilege when third parties are involved).

147 296 F.2d 918 (2d Cir. 1961).

148 Id. at 919.

149 Id. at 922.

150 Id. at 921.

151 See, e.g., *United States v. Adlman*, 68 F.3d 1495, 1499 (2d Cir. 1995) ('Under certain circumstances . . . the privilege for communication with attorneys can extend to shield communications to others when the purpose of the communication is to assist the attorney in rendering advice to the client.'); *United States v. Ackert*, 169 F.3d 136, 139 ('[T]he inclusion of a third party in attorney–client communications does not destroy the privilege if the purpose of the third party's participation is to improve the comprehension of the communications between attorney and client.'); *Exp.-Imp. Bank of the U.S. v. Asia Pulp & Paper Co.*, 232 F.R.D. 103, 113 (S.D.N.Y. 2005) (recognising, under *Kovel*, that 'communications with a financial adviser are covered by the attorney–client privilege if the financial adviser's role is limited to helping a lawyer give effective advice by explaining financial concepts to the lawyer').

privilege, if the consultant is otherwise performing a business function.[152] Instead, the company must show that the consultant's involvement was indispensable to – or served some specialised purpose in facilitating – the legal advice.[153]

For example, a client's statements to a private investigator hired by the client's attorney are often protected by the attorney–client privilege when the investigator acts as an agent of the attorney.[154] Similarly privileged (as work-product) are an investigator's interviews to gather background information for the attorney.[155] If, however, the investigator is going to be a fact witness concerning the information he or she has gathered, then all aspects of the investigator's fact gathering may be open to discovery, including statements by third parties to the investigator and the underlying factual data gathered by the investigator. Therefore, any work-product privilege that might have protected that information is waived by virtue of the private investigator's decision to testify.[156]

Courts have also extended attorney–client privilege to include public relations consultants under certain circumstances.[157] In particular, communications with public relations consultants have been found to maintain privilege if the primary purpose of the communication was to aid in the rendering of legal advice.[158] Such

152 See *In re Premera Blue Cross Customer Data Security Breach Litigation*, 296 F. Supp. 3d 1230, 1244-46 (D. Or. 2017)(declining to extend attorney–client privilege to a third party consulting firm hired in the context of a data breach, where (1) the firm began its work on the project before counsel was retained; and (2) while the firm later entered into an agreement with the law firm directly, the consulting firm's scope of work did not otherwise change); *Durling v. Papa John's International, Inc.*, No. 16 Civ. 3592 (CS) (JCM), 2018 U.S. Dist. LEXIS 11584, at *14 (S.D.N.Y. 24 January 2018) (declining to extend attorney–client privilege protection to a consultant hired to analyse how a pizza company should reimburse its delivery drivers, finding that the consultants' 'role was not as a translator or interpreter of client communications', and that the company retained the consultant 'not to improve the comprehension of the communications between attorney and client, but rather to obtain information that [the company] did not already have').

153 See, e.g., *Narayanan v. Southern Global Holdings Inc.*, 285 F. Supp. 3d 604, 611-12 (W.D.N.Y. 2018).

154 See *U.S. Dept. of Educ. v. National Collegiate Athletic Ass'n.*, 481 F.3d 936, 937 (7th Cir. 2007) (recognising that, while there is no 'private investigators privilege,' there are circumstances where attorney–client privilege can 'embrace a lawyer's agents (including an investigator).'); see also, e.g., *Clark v. City of Munster*, 115 F.R.D. 609, 613 (N.D. Ind. 1987) (finding that statements made by a defendant to a private investigator employed by his attorney are protected by attorney–client privilege.)

155 *Clark*, 115 F.R.D. at 614.

156 See *Brown v. Trigg*, 791 F.2d 598, 601 (7th Cir. 1986); *United States v. Nobles*, 422 U.S. 225 (1975) (finding that by electing to present the investigator as witness, the defendant waived his privilege as to information collected by the investigator and his attorney).

157 See *Grand Jury Subpoenas*, 265 F. Supp. 2d 321, 321 (S.D.N.Y. 2003); *Calvin Klein Trademark Trust v. Wachner*, 198 F.R.D. 53, 55 (S.D.N.Y. 2000).

158 See, e.g., *Grand Jury Subpoenas*, 265 F. Supp. 2d at 325; but see *Guiffre v. Maxwell*, No. 15 Civ. 7433 (RWS), 2016 U.S. Dist. LEXIS 58204, at *23-25 (S.D.N.Y. 2 May 2016). (Finding that the media agent's involvement in otherwise privileged communications between the defendant and her lawyer destroyed any privilege protection because the defendant failed to establish (1) 'that [the agent] was necessary to implementing [the lawyer's] legal advice;' (2) that she 'was incapable of understanding counsel's advice . . . without the intervention of a "media agent";' or

communications are found within the bounds of attorney–client privilege if the consultant provides services necessary to promote the attorney's effectiveness in the client's legal representation or the consultant is essentially an extension of the attorney under agency principles, or both.[159]

See Chapter 38 on publicity

Even with this guidance, the extent to which public relations consultants come within the bounds of attorney–client privilege is often unclear. For example, in *Calvin Klein Trademark Trust v. Wachner*, a court in the Southern District of New York refused to extend the attorney–client privilege to protect documents and testimony sought from Robinson Lerer & Montgomery (RLM), a public-relations firm retained by counsel to Calvin Klein.[160] In so ruling, the court held, *inter alia*, that the 'possibility' that communications between counsel and RLM might help counsel formulate legal advice was 'not in itself sufficient to implicate the privilege',[161] and that extending the privilege to the documents and communications at issue would apply the privilege too broadly because RLM did not appear to perform functions 'materially different from those that any ordinary public relations firm would have performed'.[162]

A few months later, in *In re Copper Market Antitrust Litigation*, a different judge from the same district court reached the exact opposite conclusion regarding the same public relations firm, finding that RLM acted as the company's 'spokesperson' when dealing with issues related to a copper trading scandal, and frequently conferred with counsel.[163] Under these facts, the court found that RLM acted as the 'functional equivalent of an in-house public-relations department with respect to Western media relations' and therefore found that the communications between RLM, the company and counsel were made for the purpose of facilitating the provision of legal advice.[164]

Similarly, in *FTC v. GlaxoSmithKline*, the US Court of Appeals for the DC Circuit found that communications with a public relations firm were protected by the privilege.[165] In so ruling, the court adopted the *Copper Market* court's rationale, crediting a party affirmation that the consultant became an 'integral member of the team assigned to deal with the issues [that] . . . were completely intertwined with [the client's] litigation and legal strategies',[166] Hence, to improve the likelihood that communications with a public relations firm will be cloaked in

(3) 'that [the agent] was translating information between [the lawyer] and Defendant in the literal or figurative sense.')

159 See *Haugh v. Schroder Inv. Mgmt. N. Am., Inc.*, No. 02 Civ. 7955 (DLC), 2003 U.S. Dist. Lexis 14586, at *8 (S.D.N.Y. 25 August 2003); *GlaxoSmithKline*, 294 F.3d at 148.

160 198 F.R.D. at 54.

161 Id.

162 Id. at 55.

163 200 F.R.D. 213, 215 (S.D.N.Y. 2001).

164 Id. at 216.

165 294 F.3d 141 (2002).

166 Id.

attorney–client privilege, the firm should interact regularly with counsel, and act as an agent at counsel's direction.[167]

In sum, a party claiming the benefit of attorney–client privilege has the burden of establishing all of the essential elements to qualify for the protections of the privilege.[168] Consequently, an attorney who wishes to consult with a non-attorney professional must seek to establish that the third party's involvement will facilitate legal advice from the beginning of the engagement.[169]

To support its claim that communications with, and documents generated by, a third party consultant are protected under the attorney–client relationship, counsel should memorialise the nature of the consultant's engagement in a *Kovel* letter. Such a letter should (1) state that counsel is retaining the consultant to assist with the provision of legal advice to the client, (2) instruct the consultant about specific tasks to be performed in support of the provision of that legal advice, (3) state that all work-product generated under the scope of the engagement is the property of counsel and (4) instruct the consultant to maintain the confidentiality of all information received or created in the course of the engagement. Further, the consultant should be guided in his or her actions by the attorney, rather than independently by the client.

Disclosure to the company's auditors 36.6.1

The disclosure of attorney–client privileged information to a company's external auditors ordinarily constitutes a subject-matter privilege waiver.[170] To the extent that counsel anticipates that the company's external auditors may require information about the status of an ongoing investigation, counsel should be prepared to communicate with auditors in a way that will limit any waiver of privilege. For example, counsel may provide the external auditor detailed information about the investigative process – including the structure, the personnel involved, the document preservation steps that were taken, general information about the process of reviewing documents and conducting interviews, and external consultants employed to assist in the investigation – which may provide the external auditors with a level of comfort about the comprehensive nature of the investigative process, without waiving the privilege regarding the substance of the investigation.

And while the disclosure of privileged information to auditors will likely waive the attorney–client privilege, work-product protection may remain intact if the auditor's interests are found not to be 'adverse' to the client. For instance, in

167 But see *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1242 (D. Or. 2017). (Declining to extend attorney–client privilege to communications with a public relations firm because 'drafting press releases relating to a security breach is a business function' and '[h]aving outside counsel hire a public relations firm is insufficient to cloak that business function with the attorney–client privilege.')

168 See *Adlman*, 68 F.3d at 1500 (finding that a party claiming protection under the attorney–client privilege has the burden of proving each of the elements of such a privilege by contemporaneous proof of a *Kovel* agreement).

169 See, e.g., *In re G-I Holdings, Inc.*, 218 F.R.D. 428, 436 (D.N.J. 2003).

170 See, e.g., *Chevron Corp. v. Pennzoil Co.*, 974 F.2d 1156, 1162 (9th Cir. 1992).

Merrill Lynch & Co v. Allegheny Energy Inc,[171] Allegheny sought to compel discovery of two internal investigation reports (prepared by counsel) that Merrill Lynch had disclosed to its auditor, arguing that the disclosure constituted a waiver of any applicable privilege.[172] The court disagreed, stating that the 'critical inquiry' is whether the auditors 'should be conceived of as an adversary or a conduit to a potential adversary'.[173] The court held that 'any tension between an auditor and a corporation that arises from an auditor's need to scrutinize and investigate a corporation's records and book-keeping practices simply is not the equivalent of an adversarial relationship contemplated by the work-product doctrine.'[174] Consistent with the *Allegheny* court's guidance, if the client cannot avoid disclosure of privileged information to its auditors, counsel may be able to argue in subsequent civil litigation that work-product protection remains intact under this principle.

36.6.2 Disclosure to foreign governments

When analysing issues of waiver surrounding productions to foreign governments, courts of the United States tend to focus on whether the production of privileged material was compelled or voluntary. Where the submission is compelled or where there was no opportunity to assert the privilege, United States courts will generally find that the privilege was not waived.[175]

36.7 Expert witnesses

Where government investigations involve complex financial transactions and other areas requiring specialised knowledge, counsel will often retain experts during the investigative stage to assist in their assessment of potential liability and in the building of the defence case. As with any external consultants, counsel should take steps to clarify that experts are being retained to assist counsel in their provision of legal advice, to maintain privilege over communications with the expert and their underlying analysis.

171 229 F.R.D. 441 (S.D.N.Y. 2004).

172 Id. at 444.

173 Id. at 447.

174 Id. at 448.

175 See *In re Grand Jury Proceedings*, 219 F.3d at 191 ('[V]oluntary (as opposed to compelled) disclosure of documents to the SEC waived the company's work-product privilege as to other parties.'); *Westinghouse Elec. Corp.*, 951 F.2d at 1427 n.14 (finding privilege waiver in subsequent litigation where the party withdrew objections to SEC subpoena production and produced documents and noting that 'had [party] continued to object to the subpoena and produced the documents only after being ordered to do so, we would not consider its disclosure of those documents to be voluntary'); *In re Vitamin Antitrust Litig.*, No. MC 99-197 (TFH), 2002 WL 35021999, at *28 (D.D.C. 23 January 2002) ('[C]ompulsion avoiding waiver requires that a disclosure be made in response to a court order or subpoena or the demand of a governmental authority backed by sanctions for noncompliance, and that any available privilege or protection must be asserted.').

In the context of a criminal action that may follow an internal investigation, unless counsel determines that it would be advantageous to present expert analysis in conjunction with a report of its investigative findings to the government or regulatory authority, consulting expert materials will otherwise remain shielded from discovery as attorney–client privileged materials. If the defence intends to call an expert witness at trial, however, counsel may be obliged – at the government's request – to provide a written summary of the testimony that the defendant intends to offer at trial.[176] And while Federal Rule of Criminal Procedure 16 contemplates that the expert's underlying memoranda and other documents created during the case investigation will remain protected from disclosure,[177] counsel will still be required to produce documents that may qualify as 'statements' of a testifying expert under Rule 26.2 prior to trial.[178]

In the context of civil litigation that may follow an internal investigation, however, expert discovery will be governed by Federal Rule of Civil Procedure 26. Prior to 2010, there was a significant risk that any documents provided to a testifying expert witness would be discoverable under Rule 26, even if they were previously considered attorney–client privileged.[179] But the 2010 amendments to the rule made significant changes that strictly limited the discovery of communications between counsel and experts, including the discovery of draft expert reports. For example, Rule 26(b)(4)(B) was added to provide work-product protection for drafts of expert reports or disclosure.[180] In addition, Rule 26(b)(4)(C) was added to provide work-product protection for attorney-expert communications.[181] These amendments to Rule 26 were designed to protect counsel's work-product and ensure that lawyers may interact with experts 'without fear of exposing those communications to searching discovery'.[182]

Although the 2010 amendments provide significant protection for expert drafts and attorney–expert communications, counsel should still make efforts to limit the scope of potential disclosure by effectively managing a testifying expert's access to information and the development of the expert's opinions. For example, Rule 26 does not preclude discovery of facts or data provided to the expert

176 See Fed. R. Crim. P. 16(b)(1)(C).

177 See Fed. R. Crim. P. 16(b)(2)(A).

178 See Fed. R. Crim P. 26.2(f) (listing 'statement[s]' of testifying witnesses to include (1) a written statement that the witness makes and signs, or otherwise adopts or approves; (2) a substantially verbatim, contemporaneously recorded recital of the witness's oral statement that is contained in any recording or any transcription of a recording; or (3) the witness's statement to a grand jury, however taken or recorded, or a transcription of such a statement).

179 See *Synthes Spine v. Walden*, 232 F.R.D. 460, 463 (E.D. Pa. 2005) (collecting cases and requiring disclosure of privileged material); see also *Galvin v. Pepe*, No. 09-cv-104-PB, 2010 WL 3092640, at *6-7 (D.N.H. 5 August 2010) (citing id.).

180 Fed. R. Civ. P. 26(b)(4) advisory committee's note.

181 Id.

182 See *Commodity Futures Trading Comm'n v. Newell*, 301 F.R.D. 348, 352 (N.D. Ill. 2014) (explaining that the government is not allowed to discover drafts of expert reports or attorney expert communications, unless communications fall within one of the three specific exceptions in Rule 26(b)(4)(C)).

by an attorney, such as fact work-product prepared for the expert by counsel.[183] Consequently, counsel should create an inventory of all factual materials provided to a testifying expert and ensure that all of such factual materials are accurate and final, and that such materials have been produced or are otherwise matters of public record. Further, where the committee notes accompanying Rule 26 extend to 'any materials considered by' an expert, counsel should ensure that all of the facts made available to a testifying expert are based upon the record in the case, rather than as the result of attorney–client privileged communications.

Finally, while the amendment to Federal Rule 26 protects drafts of expert reports from disclosure, state court rules of civil procedure may vary as to whether such drafts are discoverable. If there is any question as to whether drafts of an expert report may be discoverable, especially if the matter is pending in a jurisdiction governed by state law, it may be advisable to negotiate a stipulation that explicitly extends the protection of the Federal Rules to expert discovery.

183 Fed. R. Civ. P. 26(b)(4)(D).

37

Publicity: The UK Perspective

Edward Craven and Alex Bailin QC[1]

Overview 37.1

Publicity is an inevitable by-product of many investigations and criminal prosecutions, particularly in high-profile business crime cases. The potential adverse consequences of publicity for a corporation implicated in an investigation or prosecution – which include reputational damage, harm to relationships with customers, investors and employees, and the spurring of further investigations and interest by other investigating authorities – are self-evident and often significant.

Most individuals and corporations who find themselves caught up in an investigation or prosecution – whether as a suspect, defendant, witness or even victim – will therefore wish to limit the publication of information regarding their involvement. The extent to which English law will assist them in doing this will vary from case to case and will depend on a range of factors, including the nature of the information, the identity and status of the person seeking to restrict publicity, the nature and severity of harm that is likely to be caused if the information is published, the stage the investigation or proceeding has reached and the public interest in the underlying subject matter.

On the other hand, in some contexts a corporation may consider there is benefit in certain information about an ongoing investigation or prosecution being made public. In such cases, the corporation will need to be cognisant of the potential legal restrictions that govern the public disclosure of information regarding live investigations and criminal proceedings.

With these considerations in mind, this chapter examines the rules and mechanisms governing the publication of information about investigations and prosecutions.

1 Edward Craven and Alex Bailin QC are barristers at Matrix Chambers.

37.2 The common law principle of open justice

As a general starting point, anyone hoping to facilitate or restrict the publication of information regarding an investigation, prosecution or related civil or regulatory proceedings will need to be mindful of the central role that the common law 'open justice principle' plays in the UK legal system. This is the rule that, '[w]ith limited exceptions, the English courts administer judgment in public, at hearings which anyone may attend . . . and which the press may report.'[2] As well as the requirement that hearings should take place in public, the open justice principle also includes 'the placing into the public domain of judicial decisions . . . and the obligation to ensure that evidence or information communicated to a court is presumptively available to the public'.[3]

The English courts have described the principle of open justice as 'one of the most precious in our law'[4] and one that is founded on 'the value of public scrutiny as a guarantor of the quality of justice'.[5] It serves two principal purposes: first, 'to enable public scrutiny of the way in which courts decide cases – to hold the judges to account for the decisions they make and to enable the public to have confidence that they are doing their job properly'; secondly, 'to enable the public to understand how the justice system works and why decisions are taken'.[6] In particular, the courts have stressed that: 'it is impossible to over-emphasise the importance to be attached to the ability of the media to report criminal trials.'[7]

The requirement of open justice is not limited to proceedings that take place before criminal courts: it extends 'to all courts and tribunals exercising the judicial power of the state'.[8] It therefore applies equally to criminal and civil courts and other bodies such as the Financial Reporting Council and other regulatory and disciplinary tribunals. Nor is the open justice principle confined to proceedings that take place in public. It may in some circumstances require information about proceedings in private (i.e. proceedings which the public and press are properly excluded from) to be put into the public domain.[9] The position in relation to criminal investigations, prior to the commencement of any court proceedings, is nuanced and is considered further below.

Although it is a longstanding principle of the common law, the significance of the open justice principle 'has if anything increased in an age which attaches growing importance to the public accountability of public officers and institutions and to the availability of public officers and institutions and to the availability of information about the performance of their functions'.[10] The principle has particular

2 *Khuja v. Times Newspapers Limited* [2019] AC 161 at [12].
3 *R (DSD) v. The Parole Board of England and Wales* [2019] QB 285 at [170].
4 *R (C) v. Secretary of State for Justice* [2016] 1 WLR 444 at [1].
5 *A v. British Broadcasting Corporation* [2015] AC 588 at [26].
6 *Cape Intermediate Holdings Ltd v. Dring* [2019] 3 WLR 429 at [42], [43].
7 *R (Trinity Mirror Plc.) v. Croydon Crown Court* [2008] QB 770 at [32].
8 *Cape Intermediate Holdings Ltd v. Dring* [2019] 3 WLR 429 at [41].
9 *R (DSD) v. The Parole Board of England and Wales* [2019] QB 285 at [175].
10 *Khuja v. Times Newspapers Limited* [2019] AC 161 at [13].

implications for the ability of the media to report on court proceedings: 'Since the rationale of the principle is that justice should be open to public scrutiny, and the media are the conduit through which most members of the public receive information about court proceedings, it follows that the principle of open justice is inextricably linked to the freedom of the media to report on court proceedings.'[11]

Open justice and the European Convention on Human Rights 37.3

Although it is a creation of the common law, the open justice principle is reflected in Article 6 of the European Convention on Human Rights (ECHR), which entitles everyone to 'a fair and public hearing' of any determination of a criminal charge or civil rights and obligations. It is also reflected in the right to freedom of expression under Article 10, since 'the right to receive and impart information, which is guaranteed by article 10(1), may be engaged where measures are taken in relation to court proceedings to prevent information from becoming publicly available.'[12]

At the same time, the ECHR also contains other rights that may require the publication of information concerning individuals implicated in investigations or prosecutions to be restricted. In particular, Article 8 protects the right to respect for private and family life. Article 8 may also extend to business and company premises.[13] This right is engaged whenever anyone proposes to publish information about a person in respect of which that person has a 'reasonable expectation of privacy'. In such cases, the private information may only lawfully be published if this is a necessary and proportionate means of achieving a legitimate aim.

In addition, Article 6 provides that the press and public may be excluded from trials 'in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.'

Derogations from open justice 37.4

While the open justice principle is a jealously guarded 'constitutional principle',[14] it is not absolute. First, Parliament has enacted various statutory restrictions on the open justice principle which limit what may be reported about certain court proceedings. Second, since the open justice principle is a development of the common law, the courts have an inherent jurisdiction to determine its scope and requirements.[15] Over the years the courts have recognised a number of circumstances where derogations from the open justice principle are permitted or required. For present purposes, the most pertinent exceptions are those required to give effect to the rights under Articles 2, 3 and 8 of the ECHR.

11 *A v. British Broadcasting Corporation* [2015] AC 588 at [26].

12 *A v. British Broadcasting Corporation* [2015] AC 588 at [47].

13 *Niemietz v. Germany* (1992) 16 EHRR 97; *Société Colas Est v. France* (2002) App no 37971/91, 16 April.

14 *Cape Intermediate Holdings Ltd v. Dring* [2019] 3 WLR 429 at [41].

15 *A v. British Broadcasting Corporation* [2015] AC 588 at [27].

37.4.1 Restrictions on publicity where absolute rights are engaged

Articles 2 and 3 of the ECHR enshrine the right to life and protection from serious physical harm. The 'absolute' character of those rights means that they cannot be balanced against other 'qualified' rights such as the right to freedom of expression. Nor can they be balanced against countervailing public interests such as the importance of media reporting on court proceedings. Consequently, if the publication of certain information about an investigation or prosecution would expose an individual to a real risk of physical harm or death, then a court is required by Articles 2 and 3 of the ECHR to take effective steps to prevent that risk from materialising. (A court may, for example, make an anonymity order and take other associated procedural steps to protect the identity of a witness or party from a threat of violence arising from the proceedings.)[16] The court must, however, ensure that the extent of the interference with the media's rights is no greater than is necessary to protect against the risk of harm.[17] In civil proceedings, a variety of measures can be utilised to address such risks, including 'ring-fenced' testimony, which is heard in private and accessible only by a limited 'confidentiality club'. But such measures are necessarily more limited in criminal proceedings where the open justice principle is particularly strong and where the power to hear any part of the trial in private is very limited indeed.[18]

37.4.2 Restrictions on publicity where qualified rights are engaged

Where there is a conflict between the media's right to report on an investigation or prosecution and the Article 8 privacy rights of a person implicated in it (e.g. a defendant, suspect, witness or victim) then 'a balance must be struck, so as to ensure that any restriction upon the rights of the media, on the one hand, or of the litigants or third parties, on the other hand, is proportionate in the circumstances.'[19] In applying that balance, neither the right of the media nor the right of the individual affected by publicity has automatic precedence over the other. Instead, the court must apply 'an intense focus on the comparative rights claimed in the individual case'. The respective justifications for interfering with each right must be considered, and the proportionality of the respective interferences must be assessed.[20]

In carrying out that fact-sensitive evaluation, the court must pay close attention to the purpose of the open justice principle, the potential value of the information in question in advancing that purpose and, conversely, any risk of harm its disclosure may cause to the maintenance of an effective judicial process or to the legitimate interests of others.[21] In applying the open justice principle, the courts will generally proceed on the basis that the press 'should be trusted to fulfil

16 *In re Guardian News and Media* [2010] 2 AC 697 at [26], [27].

17 *A v. British Broadcasting Corporation* [2015] AC 588 at [49].

18 *Criminal Procedure Rules, rule 6.6; Guardian News & Media Ltd v. Incedal* [2016] EMLR 14 at [49].

19 *A v. British Broadcasting Corporation* [2015] AC 588 at [48].

20 *In re S (A Child) (Identification: Restrictions on Publication)* [2005] 1 AC 593 at [17].

21 *A v. British Broadcasting Corporation* [2015] AC 588 at [41] (adopting the test laid down in *Kennedy v. Charity Commission* [2015] AC 455 at [113]).

their responsibilities accurately to inform the public of court proceedings, and to exercise sensible judgment about the publication of comment which may interfere with the administration of justice.'[22]

Suspects in criminal investigations: before charge 37.4.3

In recent years the English courts have recognised that suspects in criminal investigations who have not yet been charged with any offence have a legitimate interest in limiting publication about their status as suspects. Whether or not there is a reasonable expectation of privacy in a criminal investigation is 'a fact-sensitive question and is not capable of universal answer one way or the other'.[23] However, 'as a matter of general principle, a suspect has a reasonable expectation of privacy in relation to a police investigation'.[24] This is because:

> *As a general rule it is understandable and justifiable (and reasonable) that a suspect would not wish others to know of the investigation because of the stigma attached. . . . If the presumption of innocence were perfectly understood and given effect to, and if the general public was universally capable of adopting a completely open- and broad-minded view of the fact of an investigation so that there was no risk of taint either during the investigation or afterwards (assuming no charge) then the position might be different. But neither of those things is true. The fact of an investigation, as a general rule, will of itself carry some stigma, no matter how often one says it should not.*[25]

There is therefore a 'clear public policy . . . that suspects in criminal investigations should not be identified prior to charge'.[26] Similarly, the courts have held that the fact that investigators have conducted a search of a suspect's property does not, without more, deprive the suspect of their legitimate expectation of privacy:

> *The circumstances of the execution of the warrant may, as a matter of practice, involve a certain compromise of the privacy of the investigation . . . but it does not follow from that that privacy rights should be automatically and totally lost. If there is a legitimate expectation of privacy before the search then the search itself would have to be carried out with a due regard to it (which is doubtless why, in practice, the police do not now identify who the subject of the search was, even if neighbours might know).*[27]

It is important to note, however, that although the 'starting point' is that a suspect has a reasonable expectation of privacy unless and until they are charged, there

22 *R v. B* [2006] EWCA Crim 2692 at [25].
23 *Sir Cliff Richard v. British Broadcasting Corporation* [2019] Ch 169 at [237].
24 Ibid., at [248].
25 Ibid.
26 *ZXC v. Bloomberg L.P.* [2019] EWHC 970 (QB) at [125].
27 *Sir Cliff Richard v. British Broadcasting Corporation* [2019] Ch 169 at [255].

may be 'all sorts of reasons why, in a given case, there is no reasonable expectation of privacy, or why an original reasonable expectation is displaced' even though a suspect has not yet been charged (for example, because there is a risk of harm to the public or because the identity of the suspect is already widely known to the public).[28] Also, the existence of a reasonable expectation of privacy is merely the starting point, and not the endpoint, of the analysis. Once a reasonable expectation of privacy has been established, the lawfulness of publishing that information will depend on whether publication is a necessary and proportionate means of pursuing some legitimate objective in the public interest.

These principles are reflected by the guidance on media relations issued by the College of Policing, which stresses that: 'The police service has a duty to safeguard the confidentiality and integrity of the information it holds and the rights of individuals to privacy.' The guidance explains:

> *Suspects should not be identified to the media (by disclosing names or other identifying information) prior to the point of charge except where justified by clear circumstances e.g. a threat to life, the prevention or detection of crime or a matter of public interest and confidence.*
>
> . . . . .
>
> *Police will not name those arrested, or suspected of a crime, save in exceptional circumstances where there is a legitimate policing purpose to do so.*[29]

The basic guidance of the Financial Conduct Authority (FCA) on publicity in criminal investigations is set out in the FCA Enforcement Guide 6.6:

> *EG 6.6 Publicity during, or upon the conclusion of criminal action*
> *EG 6.6.1 The FCA will normally publicise the outcome of public hearings in criminal prosecutions.*
> *EG 6.6.2 When conducting a criminal investigation the FCA will generally consider making a public announcement when suspects are arrested, when search warrants are executed and when charges are laid. A public announcement may also be made at other stages of the investigation when this is considered appropriate.*
> *EG 6.6.3 The FCA will always be very careful to ensure that any FCA publicity does not prejudice the fairness of any subsequent trial.*

The SFO's general guidance on the issue is as follows:

> *We try to provide as much information as we can without compromising law enforcement work, prejudicing the right of defendants to a fair trial, or causing avoidable reputational damage or harm to individuals or businesses under*

28 Ibid., at [251].

29 College of Policing guidance on media relations (May 2017), quoted in *ZXC v. Bloomberg L.P.* [2019] EWHC 970 (QB) at [122].

investigation. In practice the amount of information we can provide, particularly about cases which are in the investigation stage, is usually very limited.

Before the Director decides whether to open an investigation, the SFO does not normally confirm or deny interest in allegations made against either companies or individuals. If asked, we would normally say no more than that we are aware of the situation and that we are monitoring it.

Once the Director has formally opened a criminal investigation, the position will change in the following circumstances:

(a) the company under investigation itself makes the information public. This normally happens when a publicly listed company is informed of our investigation and considers this fact to be market-sensitive information of which it must inform the market. In such cases the SFO will (usually in co-ordination with the company's lawyers) confirm the fact and focus of the investigation after the market has been informed, or

(b) there are operational reasons for announcing the investigation (such as a call for witnesses). Or,

(c) there is some other substantial reason why the announcement of the investigation would be in the public interest.

. . . . .

Once an investigation results in a decision to prosecute and a company or an individual is charged with an offence, we announce the relevant name and charges. This may happen at the time the individual or company appears in court in answer to a requisition.[30]

Suspects in criminal investigations: after charge 37.4.4

While a suspect is likely to have a reasonable expectation of privacy prior to a charging decision, the position changes if and when they are charged: 'a person cannot ordinarily have an expectation of privacy once s/he has been charged with a criminal offence.'[31] The College of Policing's media relations guidance explains:

Those charged with an offence should be named unless there is an exceptional and legitimate policing purpose for not doing so or reporting restrictions apply. This information can be given at the point of charge.

. . . . .

If charges are withdrawn before someone first appears in court, forces should proactively release this information as soon as possible in order to be fair to the person involved, especially if a case has previously been publicised.

In practice, in the absence of any applicable statutory reporting restrictions or a real risk of death or serious injury, a person who has been charged with an

30 Serious Fraud Office, 'Our policy on making information about our cases public', https://www.sfo.gov.uk/our-cases/.

31 *ZXC v. Bloomberg L.P.* [2019] EWHC 970 (QB) at [132].

offence will be unable to prevent that information from being publicly reported by the media.

37.4.5 Persons who are named in open court

While a suspect who has not been charged with any offence is likely to have a reasonable expectation of privacy, the position is different if that person is named as a suspect or alleged perpetrator in open court. This is because the Supreme Court has held that 'there is no reasonable expectation of privacy in relation to proceedings in open court.'[32] Nonetheless, the Court also specifically contemplated that third parties (such as an arrested person who has not been charged) may apply for anonymity during the trial of another if they fear being named in open court – under common law powers, backed up with statutory reporting restrictions.[33]

Similarly, if information about a witness or victim of an offence is discussed in open court, in the absence of statutory reporting restrictions or a real risk of death or serious injury, the witness or victim is unlikely to be able to prevent the publication of that information, unless that person has obtained, in advance, anonymity from the criminal court to prevent their naming in open court during those proceedings. In this regard, the courts have acknowledged that although criminal proceedings may have a significant 'collateral impact' on non-parties, this is 'part of the price to be paid for open justice and the freedom of the press to report fairly and accurately on judicial proceedings held in public'.[34]

37.4.6 Uncharged suspects who are named in charges laid against others

There is no statutory or common law rule that requires a charge or indictment to include the names of uncharged persons accused or suspected by a prosecutor of being party to the alleged criminal activity. Such names can be supplied to the defendants without appearing on the face of the indictment. As noted above, however, once a person has been named as a suspect in open court, they lose any reasonable expectation of privacy they may otherwise have had. Accordingly, if an uncharged suspect learns that a prosecuting authority intends to name them in charges laid against another person (e.g. by naming them as an unindicted co-conspirator), they should consider taking urgent steps (including, if necessary, by seeking third-party anonymity, injunctive relief or appropriate reporting restrictions) to prevent their name being included in a publicly accessible charge sheet[35] or indictment or being read out in open court.

32 *Khuja v. Times Newspapers Limited* [2019] AC 161 at [34].

33 Ibid., at [18], [35].

34 Ibid., at [34].

35 The inclusion of information (e.g., a person's name) in a publicly accessible charge sheet or indictment is likely to be treated in the same way as if that information had been read aloud in open court.

Criminal proceedings: statutory reporting restrictions 37.5

Under English law, a number of statutory provisions automatically restrict the publication of reports on certain types of hearings or information relating to ongoing court proceedings. In addition, various other statutory provisions confer discretionary powers on the courts to impose reporting restrictions in certain situations.

Contempt of court and the 'strict liability' rule 37.5.1

Section 1 of the Contempt of Court Act 1981 (CCA 1981) establishes the 'strict liability rule', namely that 'conduct may be treated as a contempt of court as tending to interfere with the course of justice regardless of intent to do so.' The strict liability rule applies to any 'publication' that is 'addressed to the public at large or any section of the public'[36] and that 'creates a substantial risk that the course of justice in the proceedings in question will be seriously impeded or prejudiced'.[37] The rule only applies to publications made when proceedings are 'active' – which is the case if a summons has been issued or a defendant has been arrested without warrant.[38]

The upshot of these provisions is that once a suspect has been arrested or charged, no one may publish any statement to the public (or a section of the public) that creates a substantial risk of seriously prejudicing or impeding the course of justice in those proceedings. Such a risk may be created in a number of ways: for example by vilifying a suspect, by publishing prejudicial and inadmissible material (e.g. by revealing the defendant's prior criminal record) or by deterring witnesses from coming forward. No actual prejudice need be shown, merely the risk.

The strict liability rule is subject to an important exception in section 4(1) of the CCA 1981. Subject to the provisions set out below, anything said in open court in any civil or criminal proceedings (e.g. the testimony of a witness or allegations made by a defendant or prosecutor) may be published to the world at large, provided that the publication is a fair and accurate contemporaneous report of those proceedings and is published in good faith.

Section 4(2) of the CCA 1981 allows a court to order that any reporting on civil or criminal proceedings shall be 'postponed for such period as the court thinks necessary'. The power temporarily to postpone reporting only arises where this is necessary to avoid 'a substantial risk of prejudice to the administration of justice' either in those proceedings 'or in any other proceedings pending or imminent'. The power cannot be used to obtain a permanent injunction – if a person seeks permanently to prevent publication of a matter arising during trial, they will need to apply in advance under common law powers to prevent that matter from being aired in open court.

36 Contempt of Court Act 1981, section 2(2).

37 Ibid., at section 2(1).

38 Ibid., at Schedule 1.

37.5.2 Automatic reporting restrictions which the court may vary or remove

37.5.2.1 Preparatory hearings

In certain cases involving serious or complex fraud or other complex cases, the Crown Court may hold a preparatory hearing for the purpose of identifying relevant issues, assisting in the management of the trial and considering legal questions such as joinder or severance of charges.[39] Automatic reporting restrictions prohibit the publication of reports of these hearings (or related appeals) until the conclusion of the trial. A judge may, however, disapply or limit the application of those automatic reporting restrictions.[40]

37.5.2.2 Pretrial rulings in the Crown Court

Section 40 of the Criminal Procedure and Investigations Act 1996 (CPIA 1996) empowers the Crown Court to make binding rulings at pretrial hearings on 'any question as to the admissibility of evidence' and 'any other question of law relating to the case concerned.' Section 41 imposes automatic reporting restrictions that prohibit any report of a ruling made under section 40 (or proceedings on such an application) or any related varying or discharging order. The judge dealing with the application may, however, remove or limit those reporting restrictions.[41]

37.5.2.3 Applications for dismissal in the Crown Court

A defendant in an indictable-only case sent to the Crown Court may apply for the charge or charges to be dismissed on the basis that the evidence is insufficient for him or her to be properly convicted.[42] Automatic reporting restrictions prohibit any report of the existence of an unsuccessful dismissal application until the conclusion of the trial of the last defendant.[43]

37.5.2.4 Prosecution appeals

Part 9 of the Criminal Justice Act 2003 grants the prosecution various rights of appeal to the Court of Appeal in relation to a trial on indictment. This includes

39 See section 7 of the Criminal Justice Act 1987 (in relation to cases concerning serious or complex fraud) and section 29 of the Criminal Procedure and Investigations Act 1996 (in relation to other serious, complex or lengthy cases).

40 See section 11 of the Criminal Justice Act 1987 and section 37 of the Criminal Procedure and Investigations Act 1996. If the accused objects to the disapplication or limitation of those restrictions, the judge must hear representations from the accused and must only make such an order if satisfied that it is in interests of justice to do so. If an order is made, the accused's objections or representations must not be reported.

41 See section 40(3) of the Criminal Procedure and Investigations Act 1996. As with preparatory hearings, if the accused objects to the disapplication or limitation of the automatic reporting restrictions that apply to pretrial rulings, the judge must hear representations from the accused and must only permit the reporting of such a pretrial ruling if satisfied that it is in the interests of justice to do so. If an order is made, the accused's objections or representations must not be reported.

42 See paragraph 2 of Schedule 3 to the Crime and Disorder Act 1998.

43 Paragraph 3 of Schedule 3 to the Crime and Disorder Act 1998.

appeals against rulings that terminate the proceedings and evidentiary rulings that significantly weaken the prosecution case. Automatic reporting restrictions prohibit any reporting of such appeals, although once again the Court of Appeal and trial judge have a discretion to disapply this.[44]

Discretionary restrictions regarding deferred prosecution agreements 37.5.3

Under paragraph 12 of Schedule 17 to the Crime and Courts Act 2013, a court may order that the publication of information by the prosecutor shall be postponed 'for such period as the court considers necessary if it appears to the court that postponement is necessary for avoiding a substantial risk of prejudice to the administration of justice in any legal proceedings.' In *SFO v. Serco* the court exercised that power on the basis that the SFO was continuing to consider charging individuals with offences arising out of the matters that were the subject of the deferred prosecution agreement (DPA). Since the agreed statements of facts contained material by which such individuals could be identified, the court ordered that publication of the statement be postponed until a charging decision had been taken (whereupon the matter would be revisited by the court seized of those proceedings).[45] The court exercised the power for a similar reason in *SFO v. Tesco Stores Limited*.[46] Subsequently, however, all the individual defendants were acquitted, and were aggrieved that the DPA, when eventually made public, effectively identified them and accused them of conduct of which they had been found not guilty. In *SFO v. Rolls-Royce plc*[47] the DPA statement of facts was made public before the SFO had made charging decisions in respect of individuals in the investigation. The issue of third-party reputational rights in relation to DPAs is likely to be revisited in subsequent DPAs.

Appeals against derogations from open justice 37.5.4

Section 159 of the Criminal Justice Act 1988 gives a right to appeal to the Court of Appeal to any 'person aggrieved' by any order under section 4 or 11 of the CCA made in relation to a trial on indictment, any order restricting the access of the public to the whole or any part of a trial on indictment, and any order restricting the publication of any report of the whole or any part of a trial on indictment. Note, however, that a person who is aggrieved by the refusal of the court to make

See Chapter 23 on negotiating global settlements

44 See sections 62 and 63 of the Criminal Justice Act 2003.

45 *Serious Fraud Office v. Serco Geografix Limited* (Case No. U20190413) judgment of William Davis J dated 4 July 2019 at [44].

46 *Serious Fraud Office v. Tesco Stores Limited* (Case No. U20170287) [2019] EW Misc 1 (CrownC), at [110] to [114]. In addition, the court has power under section 4(2) of the CCA 1981 to postpone reporting of any hearing concerning a DPA for a period it considers necessary to avoid a substantial risk of prejudice to the administration of justice in those or in other pending or imminent proceedings.

47 *SFO v. Rolls-Royce plc* (Case No. U20170036) [2017] Lloyd's Rep FC 249.

any reporting restrictions order has no statutory appeal right: the only remedy is to seek judicial review.[48]

37.6 Public access to information and documents from criminal courts

In addition to the right to attend and report on hearings held in open court (subject to any applicable reporting restrictions) the Criminal Procedure Rules and Consolidated Criminal Practice Directions recognise the right of the public (including journalists) to obtain access to certain information or documents from court records or case materials.

Any member of the public (including a reporter) may under the Criminal Procedure Rules apply for and obtain the following information from a criminal court: (1) the date of any hearing in public; (2) each alleged offence and any plea entered; (3) any decision by the court at any hearing in public; (4) whether the case is under appeal; (5) the outcome of the case; and (6) the identity of the prosecutor, the defendants, the parties' representatives (including their addresses) and the judge or magistrate by whom a decision at a hearing in public was made.[49] In addition, upon an application by a member of the public the court may direct the provision of 'other information about the case'.[50]

Members of the public and the media may apply for access to copies of other documents referred to during court proceedings. Access will normally be granted in respect of any document that is read aloud in its entirety (or which is treated as having been read aloud in its entirety) in open court. This includes opening notes, expert reports, skeleton arguments and written decisions by the court.[51] Other documents, such as materials from the jury bundles and exhibits, may also be made available to the public and media.[52] Those principles were recently reaffirmed by the Supreme Court, which held that the default position was that the public should be allowed access not only to the parties' written submissions and arguments but also to the documents that had been placed before the court and referred to during the hearing. But a non-party would have to explain why he or she sought access and how granting access would advance the open justice principle; the court would then have to carry out a fact-specific balancing exercise by weighing the potential value of the information sought in advancing the purpose of the open justice principle against any risk of harm its disclosure might cause to the maintenance of an effective judicial process or to the legitimate interests of others.[53]

The Criminal Practice Directions provide that where an application for access is made by legal representatives instructed by the media or by an accredited

48 *R v. Marine A* [2014] 1 WLR 3326 at [31], [48].

49 Criminal Procedure Rules, rule 5.8(4),(6).

50 Ibid., at rule 5.8(7).

51 See the Consolidated Criminal Practice Directions 2015 [2015] EWCA Crim 1567 at paragraphs 5B.10 to 5B.13.

52 Ibid., at paragraph 5B.17.

53 *Cape Intermediate Holdings Ltd v. Dring* [2019] 3 WLR 429.

member of the media 'there is a greater presumption in favour of providing the requested material' and '[t]he general principle . . . is that the court should supply documents and information unless there is a good reason not to in order to protect the rights or legitimate interests of others and the request will not place an undue burden on the court.'[54] The Practice Directions add that: 'the rights of a defendant, witnesses and victims under Article 6 and 8 of the European Convention on Human Rights may also restrict the power to release material to third parties.'[55]

In addition to the right of the media and public to obtain information and court documents, a criminal court is also under a duty proactively to publish information about hearings due to be heard in public, including (1) the date, time and place of the hearing; (2) the identity of the defendant; and (3) 'such other information as it may be practicable to publish' concerning the type of the hearing, the identity of the prosecutor, the identity of the court, the offence or offences alleged and the existence of any reporting restrictions.[56]

Libel and data protection 37.7

Libel 37.7.1

An individual or corporation that is the subject of false and damaging reporting in connection with an investigation or criminal prosecution may have a claim in libel against the publisher. To establish liability for libel, a person must demonstrate that they have suffered, or are likely to suffer, 'serious reputational harm' as a result of the defamatory publication. In the case of a body that trades for profit, this requirement is only met if the publication 'has caused or is likely to cause the body serious financial loss'.[57] Under the so-called 'repetition rule', a person who reports a defamatory allegation made by another is treated as though they had made the allegation themselves.[58]

A publisher of a defamatory statement will have a complete defence if the statement is true, or if it meets the requirements of the defence of honest opinion[59] or publication on a matter of public interest.[60] In addition, a fair and accu-

54 See the Consolidated Criminal Practice Directions 2015 [2015] EWCA Crim 1567 at paragraph 5B.26, citing the judgment of the Court of Appeal in *R (Guardian News and Media) v. City of Westminster Magistrates' Court* [2013] QB 618 at [87].

55 Ibid., at paragraph 5B.24.

56 Criminal Procedure Rules, rule 5.8(10).

57 Defamation Act 2013, section 1.

58 As Lord Devlin explained in *Lewis v. Daily Telegraph Ltd* [1964] AC 234 at [284]: 'For the purpose of the law of libel a hearsay statement is the same as a direct statement, and that is all there is to it.'

59 See section 3 of the Defamation Act 2013. The requirements for this defence are, in summary, that: (1) the statement was a statement of opinion; (2) the statement indicated, whether in general or specific terms, the basis of the opinion; and (3) an honest person could have held the opinion expressed on the basis of any fact that existed at the time the statement was published or anything claimed to be a fact that was published in a privileged statement published before the statement complained of.

60 See section 4 of the Defamation Act 2013. The requirements for this defence are, in summary, that: (1) the statement complained of was, or formed part of, a statement on a matter of public interest; and (2) the defendant reasonably believed that publishing the statement complained

rate contemporaneous report of any proceedings before any court in the United Kingdom is protected by the defence of absolute privilege.[61]

It is generally difficult to obtain an interim injunction preventing a person from publishing a defamatory statement.[62] Given the potential size of a damages award for a serious libel, however, a well-founded threat to pursue libel proceedings may give a prospective publisher pause for thought before publishing potentially defamatory information.

37.7.2 Data protection

The publication of information about an identifiable living individual will constitute 'processing' of 'personal data' under the Data Protection Act 2018. Part 3 contains specific rules governing the processing of personal data by law enforcement authorities such as the police, SFO, National Crime Agency, Financial Conduct Authority and Her Majesty's Revenue and Customs. All processing of personal data for law enforcement purposes must be lawful and fair. Processing will only be lawful 'if and to the extent that it is based on law' and either the data subject has consented or the processing is 'necessary for the performance of a task carried out' by that authority. Accordingly, any decision by a lawful enforcement authority to publicise particular information about an individual's involvement in an investigation or prosecution will need to comply with these requirements.

See Chapter 40 on data protection

37.8 Public relations

Most corporations involved in a serious investigation or prosecution would be well advised to seek professional communications advice from specialist corporate communications consultants with specific expertise of managing the PR implications of criminal investigations or proceedings. Before doing so, however, it is important to be mindful that communications with such consultants are unlikely to be protected by legal professional privilege and could be the subject of compulsory production by law enforcement authorities or disclosure in related civil litigation.

See Chapters 35 on privilege and 39 on protecting corporate reputation

---

of was in the public interest. For these purposes, if the statement was part of an accurate and impartial account of a dispute that the claimant was a party to, a court determining whether it was reasonable for the defendant to believe that publishing the statement was in the public interest must disregard any omission of the defendant to take steps to verify the truth of the allegation conveyed by the statement.

61 See section 14(1) of the Defamation Act 1996. Similarly, a fair and accurate non-contemporaneous report of court proceedings in public is protected by the defence of qualified privilege at common law: see *Reynolds v. Times Newspapers Ltd* [2001] 2 AC 127 at [196] and *Kimber v. Press Association* [1893] 1 QB 65 at [68], [69].

62 As *Duncan and Neill on Defamation* (Fourth Edition) explains at paragraph 26.02, 'the general rule is that an interim injunction will not be granted in a claim for libel or slander if there is any doubt as to whether the statement is defamatory. Nor will an injunction be granted where the defendant provides a statement asserting that he will be able to prove that the statement complained of is true or that he intends to rely on another recognised defence, such as qualified privilege or honest opinion, unless it is clear that any such defence will fail at trial'.

38

Publicity: The US Perspective

Jodi Avergun[1]

The US Constitution guarantees defendants in criminal cases the right to a speedy and public trial. It also guarantees all Americans freedom of speech and freedom of the press. In the trial setting, these constitutional rights are sometimes in conflict. For instance, although freedom of the press is guaranteed, media reports about a case can taint a pool of potential jurors or might allow sworn jurors to learn about matters not in evidence. Accordingly, lawyers practising in the United States must be aware of the multiple, conflicting rights that affect judicial proceedings. These rights include the public's right of access to trial proceedings,[2] the media's right to report what occurs in court,[3] the litigants' freedom of speech[4] and

1 Jodi Avergun is a partner at Cadwalader, Wickersham & Taft LLP. The author wishes to acknowledge the contribution of Monica Martin, an associate in Cadwalader's New York office to this chapter.

2 *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 575-81 (1980) (holding that the right of the public and the press to attend criminal trials is guaranteed under the First and Fourteenth Amendments, and that, absent an overriding interest established after a factual hearing, the trial of a criminal case must be open to the public). In 1986, the US Supreme Court extended its ruling in *Richmond Newspapers* to jury selection. *Press-Enterprise Co. v. Superior Court of California*, 478 U.S. 1 (1986).

3 *Estes v. State of Tex.*, 381 U.S. 532, 541–42 (1965) ('Reporters of all media, including television, are always present if they wish to be and are plainly free to report whatever occurs in open court through their respective media.').

4 *Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1074-75 (1991) (describing the bounds to which limitations may be placed on a lawyer's First Amendment right to free speech).

the defendant's right to a fair trial.[5] No one right is absolute, and each is limited by various rules and regulations.[6]

A lawyer's ethical obligations, for example, may limit the attorney's First Amendment right to speak publicly about a case. Under the American Bar Association Model Rules of Professional Conduct, which have been adopted, in whole or in part, by the vast majority of US jurisdictions, a lawyer who has or is participating in a matter must not make an 'extrajudicial statement' that 'will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter'.[7] In federal criminal cases, prosecutors must also comply with these rules, as well as those published in the Justice Manual, which limits the information a prosecutor may disclose or the issues he or she may comment on.[8]

Apart from the rules prohibiting a lawyer from publicly commenting on a pending case, a lawyer's professional duty to keep client matters confidential may also prevent him or her from publicising information about a case.[9]

38.1.2 Investigatory and pretrial stage

During the investigative stage of the case, before charges have been filed, a court cannot limit an individual involved in an investigation from making public statements about the case. But because such statements can be used by a prosecutor against a defendant in a subsequent criminal proceeding (either as substantive evidence or to demonstrate that the individual waived his or her right to remain silent), lawyers often counsel their clients to exercise their free speech rights carefully, if at all. Prosecutors are more constrained, however. The Justice Manual provides that a prosecutor cannot make public statements about a case if there is substantial likelihood that the statement will materially prejudice an adjudicative proceeding.[10] Similarly, prosecutors, but not individual witnesses, are prohibited from disclosing any matters that occur before a grand jury.[11] Once charges have been filed, however, courts have greater ability to insulate their proceedings

5 *Press-Enter. Co. v. Superior Court of California, Riverside Cty.*, 464 U.S. 501, 508 (1984). ('No right ranks higher than the right of the accused to a fair trial.')

6 See *United States v. Gerena*, 869 F.2d 82, 85 (2d Cir. 1989). ('The district court must balance the public's right of access against the privacy and fair trial interests of defendants, witnesses and third parties.'); *United States v. Rajaratnam*, 708 F. Supp. 2d 371, 374 (S.D.N.Y. 2010) (explaining that '[c]ourts must balance the right [to access criminal proceedings] against other important values, like the Sixth Amendment right of the accused to a fair trial').

7 Model Rules of Prof'l Conduct R. 3.6(a) (2019).

8 U.S. Dep't of Justice, Justice Manual, § 1-7.000 (Confidentiality and Media Contacts Policy), available at https://www.justice.gov/jm/jm-1-7000-media-relations.

9 See, e.g., *Sealed Party v. Sealed Party*, No. 04-2229, 2006 U.S. Dist. LEXIS 28392 (S.D. Tex. 4 May 2006) (finding breach of fiduciary duty where attorney published a press release disclosing the terms of a confidential settlement).

10 U.S. Dep't of Justice, Justice Manual, § 1-7.000 (Confidentiality and Media Contacts Policy), available at https://www.justice.gov/jm/jm-1-7000-media-relations.

11 Rule 6(e)(2) prohibits a grand juror, interpreter, court reporter, operator of a recording device, person who transcribes recorded testimony, attorney for the government, or person to whom a proper disclosure is made under Rule 6(e)(3)(a)(ii) or (iii) from disclosing a matter occurring

from the prejudicial effects of any publicity.[12] A judge's failure to exercise this power may, under certain circumstances, violate a defendant's right to a fair trial.[13] In widely publicised cases, the local rules may authorise the court to issue orders governing extrajudicial statements by parties, witnesses and attorneys, and the seating and conduct of spectators, as well as the sequestration of jurors and witnesses.[14] Sometimes, litigants can attempt to prevent the public disclosure of private or prejudicial information prior to trial by filing their documents under seal and pursuant to protective orders.[15] However, because the First Amendment guarantees the public's right of access to governmental proceedings, sealed filings can only be made with the court's permission and upon a showing of necessity or that unfair prejudice might result from public dissemination. Accordingly, motions to seal proceedings are not lightly granted, and government lawyers in particular are severely limited in their ability to file motions under seal or to consent to their opponent's request to close proceedings.[16] Rather than seal proceedings or files, courts must consider whether a change of venue, jury sequestration or gag orders, among other techniques, would adequately protect the rights of the parties. For example, Judge Amy Berman Jackson, the judge presiding over the criminal case against President Donald Trump's former campaign manager, Paul Manafort, issued a gag order in the trial, barring anyone involved in the case from making public statements that might taint it. In her written order she stated that she wanted to make sure the trial was fair and that potential jurors were not influenced by pretrial publicity.[17] Upon a showing that pretrial publicity about the case will prevent the empanelment of an impartial jury or will otherwise

---

before the grand jury. Fed. R. Crim. P. 6(e). The rule does not impose any obligation of secrecy on witnesses.

12 See, e.g., *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539 (1976) (holding that a court may enter a 'gag' order prohibiting the reporting of evidence adduced at an open preliminary hearing if it finds 'a clear and present danger that pre-trial publicity could impinge upon the defendant's right to a fair trial').

13 *Sheppard v. Maxwell*, 384 U.S. 333 (1966) (holding that failure of a state trial judge to protect the defendant in a murder prosecution 'from the inherently prejudicial publicity which saturated the community and to control disruptive influences in the courtroom' deprived the defendant of a fair trial consistent with the Due Process Clause of the Fourteenth Amendment).

14 See, e.g., L. Cr. R 57.7(c): S.D.N.Y. L. Cr. R 23.1(h).

15 *Johnson v. Greater Se. Cmty. Hosp. Corp.*, 951 F.2d 1268, 1277 (D.C. Cir. 1991) (noting that, in permitting a party to file a document under seal, should consider '(1) the need for public access to the documents at issue; (2) the extent to which the public had access to the documents prior to the sealing order; (3) the fact that a party has objected to disclosure and the identity of that party; (4) the strength of the property and privacy interests involved; (5) the possibility of prejudice to those opposing disclosure; and (6) the purposes for which the documents were introduced'); see also *Strauss v. Credit Lyonnais, S.A.*, No. 06-CV-702, 2011 WL 4736359, at *4 (E.D.N.Y. 6 October 2011) (approving a protective order that governs the filing of documents under seal as well as the public filing of documents).

16 28 C.F.R. §50.9.

17 *United States of America v. Manafort et al.*, No. 1:17-CR-00201-ABJ (D.D.C. filed 8 November 2017), ECF No. 38.

prejudice the defendant, the defendant can move to have the case transferred to another district.[18]

38.1.3 Trial and post-trial stage

Because the right to an impartial jury is also guaranteed by the US Constitution,[19] a defendant may question jurors about their exposure to pretrial publicity.[20] In one of the most highly publicised cases in modern history – the 1995 murder trial of football legend O J Simpson – it took nearly two months to seat an impartial jury not prejudiced by the near-constant media coverage of the case. During jury selection, jurors were prohibited from reading the papers, watching television or even awakening to a clock radio.[21] In widely publicised cases, courts frequently permit lawyers additional peremptory challenges (beyond the number normally allowed), which allow lawyers to summarily disqualify a potential juror without providing a reason to the court.[22] During the trial, jurors may be sequestered to protect them from the prejudicial effect of media reporting.[23] In this day and age, the court may instruct jurors not to read or post information about the trial on social media and other internet forums.[24] A failure to allow for a fair trial or to protect the impartiality of a jury will result in a mistrial.[25]

---

18 Fed. R. Crim. P. 21(a); see also *Sheppard*, 384 U.S. at 363 (requiring the defendant to show 'a reasonable likelihood that prejudicial news prior to trial will prevent a fair trial').

19 U.S. Const. amend. VI.

20 *United States v. Blanton*, 719 F.2d 815 (6th Cir. 1983) (holding that the court produced an impartial jury and fair trial by, at voir dire, through 'extensive questioning concerning prior media impact and juror associations, coupled with many dismissals based on even hints of possible prejudice, . . . very substantial increases in the number of peremptory challenges available to each defendant . . . [and] reliance on defendants' use of detailed questionnaires concerning all potential jurors coupled with sensitive responses by the court to any of defendants' challenges arising from such use').

21 http://law2.umkc.edu/faculty/projects/ftrials/Simpson/Simpsonchron.html.

22 See, e.g., *United States v. Campa*, 459 F.3d 1121, 1135 (11th Cir. 2006) (noting that the district court twice granted the defendants' requests for additional peremptory challenges due to the publicity regarding the trial).

23 See, e.g., *United States v. Cacace*, 321 F. Supp. 2d 532, 536 (E.D.N.Y. 2004) (partly sequestering the jurors in a murder trial to reduce the risk that they may be prejudiced against the defendant, the acting boss of the Colombo crime family, by exposure to press reports of both charged and uncharged murders); *Geders v. United States*, 425 U.S. 80, 87 (1976). ('The judge's power to control the progress and, within the limits of the adversary system, the shape of the trial includes broad power to sequester witnesses before, during, and after their testimony.') The decision whether to sequester jurors is within the 'sound discretion' of the district court; e.g., *United States v. Porcaro*, 648 F.2d 753 (1st Cir. 1981).

24 See, e.g., *Bushmaker v. A. W. Chesterton Co.*, No. 09-CV-726-SLC, 2013 WL 11079371, at *12 (W.D. Wis. 1 March 2013) (instructing the jury not to post on Twitter or Facebook); Judicial Conference Committee, Proposed Model Jury Instructions: The Use of Electronic Technology to Conduct Research on or Communicate About a Case (June 2012), available at www.uscourts.gov/file/18041/download.

25 e.g., *Pearson v. Rock*, No. 12-CV-3505, 2015 WL 4509610, at *2 (E.D.N.Y. 24 July 2015) (granting a mistrial after concluding that the jury had been 'incurably tainted').

Discovery of internal corporate communications 38.1.4

Issues of public access affect other areas of legal practice. Even where confidentiality of process and information is assumed, rules governing discovery in civil or criminal cases can lead to the disclosure of internal communications and records, even in sensitive investigations. The Federal Rules of Civil Procedure allow for pretrial discovery that is far more expansive compared to other jurisdictions.[26] Specifically, Rule 26(b)(1) allows parties to conduct discovery of 'any non-privileged matter that is relevant to any party's claim or defense and proportional to the needs of the case'.[27] As a result, companies that find themselves subject to class-action or shareholder derivative lawsuits that result from internal investigations are often forced to hand over troves of potentially damaging internal corporate communications. For example, the shareholder derivative litigation against the board of the Walt Disney Company lasted more than eight years, and the extensive discovery produced a damaging factual record about the board's corporate governance practices that ultimately forced Disney CEO and board member Michael Eisner to resign.[28]

Civil discovery is not the only means through which seemingly confidential internal communications and records can become public. Many companies are forced to initiate or expand the scope of internal investigations after a regulator issues a subpoena or civil investigative demand for internal records. Additionally, certain public institutions, such as colleges and universities, are subject to public records laws that may require the institutions to release or publish documents both during and after the investigation.[29] And, increasingly, large-scale document leaks thrust internal corporate documents into the public sphere without warning.[30] The practical reality is that any organisation undergoing an internal investigation must prepare for the possibility that it will have to produce internal documents at some point.

See Chapter 11 on production of information to authorities

26 See, e.g., Stephan N Subrin, Discovery in Global Perspective: Are We Nuts?, 52 DePaul L. Rev. 299 (2002).

27 Fed. R. Civ. P. 26(b)(1).

28 Érica Gorga and Michael Halberstam, Litigation Discovery and Corporate Governance: The Missing Story About the 'Genius of American Corporate Law', 63 Emory L.J. 1383, 1401-1405 (2014).

29 In 2014, after the University of North Carolina at Chapel Hill released a public report of an investigation into academic irregularities at the university, media organisations made requests through the North Carolina Public Records Law for the nearly 1.7 million electronic records that were collected and analysed during the investigation. The University of North Carolina at Chapel Hill, 'University reports final expenses to bring NCAA and related issues to a close', (13 August 2018), http://carolinacommitment.unc.edu/updates/university-responds-to-public-records-requests-for-legal-communications-firm-expenses/.

30 For example, in 2007, an employee at HSBC Suisse surreptitiously downloaded client data from approximately 30,000 accounts and provided that data to French authorities. A portion of these files were then obtained through an international collaboration of news outlets and published in 2015 by the International Consortium of Investigative Journalists. See David Leigh et al., 'HSBC files show how Swiss bank helped clients dodge taxes and hide millions', *The Guardian*, 8 February 2015, https://www.theguardian.com/business/2015/feb/08/hsbc-files-expose-swiss-bank-clients-dodge-taxes-hide-millions?CMP=share_btn_tw.

Although a detailed description of all the defensive measures available to companies is beyond the scope of this chapter, a basic list should include confidentiality agreements to cover sensitive communications with third parties, protective orders (where available) to limit the scope and permitted usage of produced materials, and the careful maintenance of the attorney–client and work-product privilege during investigations.

See Chapter 36 on privilege

38.1.5 Consulting a public relations expert

Given the likelihood that the public may become aware of internal corporate communications relating to an investigation, many organisations (and some well-resourced individuals) resort to hiring a public relations expert to assist counsel during the course of an investigation. Public relations experts can serve a variety of functions, including preparing executives for public appearances during investigations, developing communications strategies around key investigation events (e.g., press conferences regarding investigation status), and planning for potential crises (e.g., a witness leaking the preliminary findings of an investigation prior to the investigation's completion). For many organisations, hiring a public relations expert to advise them during an internal investigation can be a foregone conclusion in the relentless 24-hour news cycle. Volkswagen, for example, hired three public relations firms based in three different countries to advise during its investigation of alleged emissions cheating.[31] During an investigation into potential corporate misconduct, special considerations arise when the public relations specialist works closely with legal counsel for the company. Frequently, questions of whether the attorney–client privilege applies to protect communications between lawyers and public relations experts arise during an investigation. Although the attorney–client privilege normally requires that the protected communication occur between a lawyer and his or her client and exclude third parties, in some circumstances the privilege extends to communications between a non-lawyer consultant and the lawyer's client. In *United States v. Kovel*, for example, the Second Circuit held that communications from the client to a consultant are privileged if they are made in confidence and 'for the purpose of obtaining legal advice'.[32]

Kovel, however, does not create a blanket privilege to protect communications between attorneys, their clients and public relations experts. Instead, after *Kovel*, courts determining whether to apply the attorney–client privilege to communications with consultants such as public relations experts have focused on whether the communications with the consultant were 'imparted in connection with the

31 Danny Hakim, 'VW's Crisis Strategy: Forward, Reverse, U-Turn', *N.Y. Times*, 26 February 2016, available at http://www.nytimes.com/2016/02/28/business/international/vws-crisis-strategy-forward-reverse-u-turn.html.

32 296 F.2d 918, 922 (2d Cir. 1961) (protecting the communications from an accountant to the client that were made in confidence for the purpose of obtaining legal advice from the lawyer, not for the purpose of obtaining the accountant's advice).

legal representation'.[33] For example, when Martha Stewart and her attorneys hired public relations consultants to assist them in dealing with the media in her high-profile insider trading case, the court protected those communications under the attorney–client privilege because the communications were made for the purpose of giving or receiving advice directed at handling Stewart's legal problems.[34] Applying *Kovel*, the court explained:

> *[T]his Court is persuaded that the ability of lawyers to perform some of their most fundamental client functions – such as (a) advising the client of the legal risks of speaking publicly and of the likely legal impact of possible alternative expressions, (b) seeking to avoid or narrow charges brought against the client, and (c) zealously seeking acquittal or vindication – would be undermined seriously if lawyers were not able to engage in frank discussions of facts and strategies with the lawyers' public relations consultants.*[35]

In contrast, the court in *Haugh v. Schroder Investment Management* found that the attorney–client privilege did not apply to a public relations expert retained for the plaintiff when the plaintiff could not show that the expert's services were 'anything other than standard public relations services' for the client, and were not necessary for plaintiff's counsel to provide the plaintiff with legal advice.[36] The conclusion to be drawn from these two cases is simple. To cloak communications with public relations experts advising clients in legal matters, the lawyer needs to retain the public relations expert, and the communications between the consultant and the client must be intended to assist the attorney in advising his or her client.

See Chapter 39 on protecting corporate reputation

Social media and the press 38.2

Social media as an investigatory tool and as evidence 38.2.1

For better or for worse, social media is more than just a tool for friends and family to connect and communicate. The prevalence of social media has created a continuously updated record that is increasingly used to investigate wrongdoing and that can be admitted as evidence in judicial proceedings.

With respect to investigative activities, whether by the government or private parties, social media users generally do not have an expectation of privacy.[37] However, some of the typical features of social media – for example, the fact

33 *United States v. Schwimmer*, 892 F.2d 237, 243 (2d Cir. 1989).

34 *In re Grand Jury Subpoenas*, 265 F. Supp. 2d 321 (S.D.N.Y. 2003).

35 Id. at 330.

36 No. 02-CIV- 7955, 2003 U.S. Dist. LEXIS 14586, at *8 (S.D.N.Y. 25 August 2003) ('Plaintiff has not shown that Murray was "performing functions materially different from those that any ordinary public relations" advisor would perform.'); see also *Scott v. Chipotle Mexican Grill*, 94 F. Supp. 3d 585 (S.D.N.Y. 2015) (holding a factual report from a human resources consultant to employer's counsel was not protected by attorney–client privilege because the employer did not show that it or counsel engaged consultant for anything more than factual research and to assist employer in making a business decision).

37 *U.S. v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004).

that social media users generally have password-protected accounts and various privacy settings to control what information other users can view – have created some legal distinctions. Courts have distinguished between public and non-public postings and focused on a user's privacy settings when determining whether Fourth Amendment protections against unreasonable searches extend to social media content accessed by the government.[38] However, even where a user limited viewable postings to his or her 'friend network', the government is not precluded from seeking co-operation from one of the user's friends authorised to view the user's content.[39] Unlike investigators, private American lawyers are constrained by ethical rules in their use of social media. For example, the New York State Bar Association's Committee on Professional Ethics has ruled that 'friending' an investigatory target or opposing party, or instructing a third party to do so on the lawyer's behalf, is a prohibited act of deceptive conduct or making of a false statement.[40] Accordingly, for private lawyers, care needs to be taken in how social media content is collected and used.

From the standpoint of admissibility as evidence in a proceeding, social media content is not fundamentally different from other paper or electronic evidence. The same evidentiary considerations apply: to be admissible, the evidence must be relevant, have probative value outweighing its potential to unfairly prejudice, and be authentic and free of hearsay.[41] Some courts treat evidence from social media similarly to other types of evidence and require only a threshold showing of authenticity.[42] Other courts require evidence that affirmatively disproves the possibility that evidence from social media was sent or manipulated by anyone other than its putative creator.[43]

38.2.2 Social media and the jury

In jury trials, issues surrounding social media generally fall into two categories: lawyers using social media to screen potential jurors, and jurors using social media improperly during a proceeding.

In the pretrial process, lawyers are ethically permitted to screen jurors based on social media profiles. On 24 April 2014, the American Bar Association issued Formal Opinion 466, which clarified that the act of passively observing a potential juror's public social media information is not improper *ex parte* contact with a juror or potential juror.[44] However, a lawyer may not send an invitation or request

38 See e.g., *People v. Harris*, 949 N.Y.S.2d 590, 592 (N.Y. Crim. Ct. 2012).

39 See e.g., *U.S. v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012).

40 Robert H Giles and Jason I Allen, "Will You Be My Friend?" – Ethical Concerns for Prosecutors and Social Media, Child Sexual Exploitation Program Update (National District Attorneys Association), 9 to 12 October 2012, at 2, available at http://www.ncdsv.org/images/NDAA-CSPE_WillYouBeMyFriend_2012.pdf.

41 See generally Fed. R. Evid. Authentication of evidence from social media is generally the biggest hurdle for admission, and two approaches are predominant.

42 See, e.g., *Tienda v. State*, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012).

43 See, e.g., *Griffin v. Maryland,* 19 A.3d 415, 423-24 (Md. 2011).

44 ABA Comm. on Prof'l Ethics & Grievances, Formal Op. 466 (2014).

to friend or connect with a potential juror to gain access to the potential juror's information. Social media websites that provide notifications to users when their information is viewed, such as LinkedIn, also do not constitute improper contact as long as the lawyer does not make an active request to view non-public information.[45] If defence counsel learns from internet research that a prospective juror has made misrepresentations during *voir dire*, counsel should bring this misconduct to the court's attention. Failure to do so could potentially result in a waiver and an impairment of the defendant's right to an impartial jury.[46]

During trial, jurors' use of social media presents a risk of mistrial. To address this risk, counsel may request jury instructions on the use of social media prior to commencement of trial. Formal Opinion 466 also suggests that courts deliver jury instructions on the use of social media 'early and often' and even 'daily in lengthy trials'.[47] This guidance comes as jurors have used social media to publicly discuss trial issues or access witnesses and litigants, which ultimately has resulted in remands, reversals and other judicial inefficiencies.

For example, in *Dimas-Martinez v. State*, a death row inmate's murder conviction was reversed and remanded, in part because of a juror's tweets during trial.[48] The jury received instructions at the beginning of the trial warning them not to tweet or use social media but a juror nonetheless tweeted at the conclusion of the evidence in the sentencing phase of the trial.[49] The defendant's lawyer notified the court, and the court questioned the juror.[50] The juror admitted to the tweet and promised to discontinue use of social media for the duration of the trial.[51] But even though the juror tweeted at least two more times, the trial court refused a motion for a new trial, finding that the defendant suffered no prejudice from the tweets.[52] The Supreme Court of Arkansas disagreed, concluding that the juror's tweets were impermissible public discussion of the case, and that the insubordination of the juror to the court's instructions contributed to the defendant's denial of a fair trial.[53]

45 Id.

46 See *United States v. Parse*, 789 F.3d 83, 114 (2d Cir. 2015) (holding that defence counsel did not knowingly waive the defendant's right to an impartial jury where, even though a Westlaw report indicated a juror may have in fact been a suspended attorney with the same name, the juror 'lied [so] comprehensively in *voir dire* and "presented herself as an entirely different person"' that defence counsel could have reasonably relied on her representations).

47 Id.

48 385 S.W.3d 238 (Ark. 2011).

49 Id. at 247-48.

50 Id. at 246.

51 Id. at 246-47.

52 Id. at 247.

53 Id. at 249.

38.3 Risks and rewards of publicity

38.3.1 Risks

High-profile criminal cases often generate media attention. And while courts may adopt judicial measures to limit the adverse effects of publicity, it may become so pervasive that it prejudices jurors' opinions regarding the question of guilt. In such cases, a court may declare a mistrial to protect the defendant's Sixth Amendment guarantee to have his or her case decided by an impartial jury.[54]

High-profile investigations spark widespread media coverage, not all of which may be accurate. In 2017, Robert Mueller was appointed as Special Counsel in a widely covered investigation into Russian interference into the 2016 US presidential election.[55] The investigation was widely reported on in the media. In one instance, BuzzFeed reported a story alleging that President Trump had directed his personal attorney Michael Cohen to lie on the president's behalf. The Special Counsel's office issued a statement in response saying that BuzzFeed's description of the events were inaccurate.[56] The investigation was plagued with allegations of inaccurate reporting, prompting the Special Counsel's office to issue a warning to reporters that, 'many stories about [the] investigation have been inaccurate'.[57]

In other extraordinary situations, defence attorneys may face disciplinary measures – the most severe of which is disbarment – for improperly engaging the media in a manner that prejudices the proceedings.[58] Prosecutors are held to a higher standard than civilian attorneys under the professional rules.[59] For example, in June 2007, Michael B Nifong, the North Carolina prosecutor who pursued a false accusation of sexual assault against three Duke University lacrosse players, was disbarred by the State Bar Disciplinary Commission for making inflammatory statements to the media in violation of Rules 3.6 and 3.8(f) of the State Bar's Rules of Professional Conduct, among other violations.[60]

---

54 See *Sheppard*, 384 U.S. at 363; see also *Arizona v. Washington*, 434 U.S. 497, 505-06 (1978) (mistrial is reserved for those special cases in which there is a 'manifest necessity').

55 Rebecca R Ruiz and Mark Landler, 'Robert Mueller, Former F.B.I. Director, Is Named Special Counsel for Russia Investigation,' *N.Y. Times* (17 May 2017) available at https://www.nytimes.com/2017/05/17/us/politics/robert-mueller-special-counsel-russia-investigation.html.

56 Devlin Barrett, Matt Zapotosky and Karoun Demirjian, 'In a rare move, Mueller's office denies BuzzFeed report that Trump told Cohen to lie about Moscow project' *N.Y. Times* (18 January 2019), available at https://www.washingtonpost.com/world/national-security/2019/01/18/b9c40d34-1b85-11e9-8813-cb9dec761e73_story.html.

57 Kieran Corcoran, 'Robert Mueller warns that "many stories about our investigation have been inaccurate"', *Business Insider* (12 April 2018), available at https://www.businessinsider.com/robert-mueller-warns-many-stories-on-trump-investigation-not-true-2018-4?r=UK.

58 See, e.g., Model Rules of Prof'l Conduct R. 3.6 (Trial Publicity) (prohibiting a lawyer from making an 'extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter').

59 See, e.g., Model Rules of Prof'l Conduct R. 3.8(f) (Special Responsibilities of a Prosecutor) (prohibiting a prosecutor from making extrajudicial comments that have a 'substantial likelihood of heightening public condemnation of the accused').

60 Id.

Unpopular defendants can face extraordinary difficulties in managing publicity while seeking an impartial hearing, which can increase both the cost and complexity of the defence. An example of this situation is the prosecution of Martin Shkreli, a former pharmaceutical CEO and hedge fund manager who was convicted of securities and wire fraud violations stemming from losses suffered by investors in his funds and companies.[61] Prior to his arrest, as the then CEO of Turing Pharmaceuticals, Mr Shkreli unapologetically raised the price of a life-saving drug by 5,000 per cent[62] and became known in the media as 'the most hated man in America'.[63] Mr Shkreli's notoriety generated daily news coverage of his subsequent federal trial which, combined with his ill-advised attempts to personally manage the publicity, required the trial judge to issue orders addressing the media's and Mr Shkreli's potential influence on the jury.[64] Mr Shkreli was convicted on two counts of securities fraud and one count of conspiracy to commit securities fraud.[65]

Civil defamation claims may also follow highly publicised cases. When numerous women accused actor and comedian Bill Cosby of sexual assault, Mr Cosby and his team publicly denied the allegations and accused the women of lying.[66] Several of the alleged victims filed civil defamation suits against Mr Cosby. A federal judge in Pennsylvania dismissed one of the suits on the basis that Mr Cosby's statements did not support a claim for defamation under state law,[67] while Mr Cosby settled a defamation suit that was pending in federal court in Massachusetts.[68]

---

61 Superseding Indictment, *United States v. Shkreli*, No. 1:15-cr-637 (E.D.N.Y. 3 June 2016), ECF No. 60.

62 Andrew Pollack, 'Drug Goes from $13.50 a Tablet to $750, Overnight', *N.Y. Times*, 20 September 2015, available at https://www.nytimes.com/2015/09/21/business/a-huge-overnight-increase-in-a-drugs-price-raises-protests.html.

63 Phil McCausland, 'Fraud Trial for Martin Shkreli, "Most Hated Man in America", Begins Monday', *NBC News*, 25 June 2017, available at https://www.nbcnews.com/news/us-news/fraud-trial-martin-shkreli-most-hated-man-america-begins-monday-n776581.

64 Docket Order, *United States v. Shkreli*, No. 1:15-cr-637 (E.D.N.Y. 5 July 2017) (following Mr Shkreli's courthouse visit with reporters covering his trial, when he remarked on evidence and the credibility of a witness, prosecutors moved for a gag order to prohibit Mr Shkreli from making any public statements about the case. Two days later, the court issued a limited gag order prohibiting Mr Shkreli from making 'comments to the press regarding the case, evidence or witnesses within the courthouse or the courthouse perimeter . . .').

65 Verdict, *United States v. Shkreli*, No. 1:15-cr-637 (E.D.N.Y. 4 August 2017), ECF No. 305.

66 See Mike Nunez, 'Bill Cosby to FLORIDA TODAY: I won't mention allegations', *Florida Today*, 22 November 2014, available at http://www.floridatoday.com/story/news/local/2014/11/21/bill-cosby-to-florida-today-i-wont-mention-allegations/19367957/.

67 *Hill v. Cosby*, No. 15-1658, 2016 U.S. Dist. LEXIS 7300 (W.D. Pa. 21 January 2016).

68 *Green v. Cosby*, No. 3:14-cv-30211 (D. Mass. filed 10 December 2014).

38.3.2 Rewards

When properly executed, tactical media coverage during an investigation or trial can counter negative public impression and alleviate prosecutorial pressure to bring charges. The public relations consultants hired by Martha Stewart in connection with her insider trading case focused narrowly on neutralising the media coverage that reached the prosecutors and regulators responsible for charging decisions so that they could make their decisions without 'undue influence from the negative press coverage'.[69] In ruling on the attorney–client privilege afforded to certain communications among Stewart, her attorneys and the public relations firm, the Court recognised the necessity of developing a communications plan in high-profile cases:

> *Just as an attorney may recommend a plea bargain or civil settlement . . . so too an attorney may take reasonable steps to defend a client's reputation and reduce the adverse consequences of indictment . . . . A defense attorney may pursue lawful strategies to obtain dismissal of an indictment or reduction of charges, including an attempt to demonstrate in the court of public opinion that the client does not deserve to be tried.*[70]

Given the importance of advocating outside the courtroom, it may also be beneficial for an attorney to exercise the right to reply under the Model Rules of Professional Conduct. Notwithstanding the prohibition at Rule 3.6(a) against extrajudicial statements that are substantially likely to materially prejudice a fair trial, Rule 3.6(c) permits a lawyer to make extrajudicial statements that protect a client from the 'substantial undue prejudicial effect' of recent publicity that was not initiated by the lawyer or the client to the extent that they are necessary to mitigate the adverse publicity.

69 *In re Grand Jury Subpoena*, 265 F. Supp. 2d at 323-324.

70 Id. (quoting *Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1043 (1991) (Kennedy, J, plurality opinion)).

39

Protecting Corporate Reputation in a Government Investigation

Kevin Bailey and Charlie Potter[1]

Introduction 39.1

Long gone are the days where remaining passive and silent while your client is dissected during a high-profile government investigation was the only sensible approach. You need look no further than the steady stream of such inquiries over the past three to five years to see that persuasive, careful communications – in conjunction with the legal strategy – are the soundest way to preserve and rebuild a company's reputation during a crisis and afterwards.

Of course, no two investigations are the same, and approaches to handling communications around them will inevitably differ according to, among other things, the jurisdictions involved, their media and political culture, and the particular agenda of the investigating authorities. So advice on communications strategy, just like legal advice, must be tailored to the circumstances.

Regardless of the tactics employed, the central objective of both lawyers and communicators is to achieve as successful an outcome to an investigation as possible, namely one that minimises lasting damage to a company's financial position, its reputation and 'licence to operate', and its brand and wider commercial standing. Communicators can work effectively with lawyers to respond to increasingly assertive and sophisticated strategies deployed by government entities, particularly since the financial crisis of 2008.

In that context, some overarching principles can be distilled from the practical experience of acting for companies faced with corporate investigations and crises. These principles are discussed in the pages that follow, addressing the need for close collaboration between communicators and lawyers on worst-case scenarios,

1 Kevin Bailey and Charlie Potter are partners at Brunswick Group LLP. The authors would like to thank Andrew Garfield, their former partner at Brunswick, for his assistance with this chapter.

planning for and executing disclosures about such investigations, the importance of keeping key stakeholders advised as much as possible, and the critical aspects of managing the endgame of an investigation.

See Chapters 37 and 38 on publicity

39.2 Planning for the worst

The right strategy for managing reputational impact through an investigation depends on a range of factors: the nature of the behaviour under investigation, the authority conducting it, the brand profile of the company, the industry in which it operates and any damage to the public or consumers.

Moreover, the history of every company is different, and how an investigation will play out in many cases turns on how it is perceived as a corporate and social actor. Is the fact of an investigation into, say, corruption allegations a complete surprise because of the company's sterling reputation, or will it be seen as the latest misstep of a recidivist? Equally important is appreciating the context of the investigation itself and whether, for instance, it may be enhanced, or even motivated, by the political agenda of a given government entity.

While understanding and appreciating these factors is critical to developing a successful communications strategy in the context of a particular investigation, one principle cuts across the approach to any investigation. In each case, companies that have planned ahead by developing and testing crisis communications plans fare better than those who have not. That is especially true where a company is involved in (and required to respond to) a dramatic, sudden, visually striking or fatal operational disaster, for example, an aeroplane crash or industrial accident, that subsequently triggers an investigation. But it applies equally to the unforeseen announcement of an investigation into issues, behaviour or incidents that may not have been in public view. These are all business-critical events. Knowing what to say and which lawyers and communications professionals to call in those first hours may be the difference between dealing with one crisis (the original incident) and several (the incident plus making up for legal and communications missteps taken in the heat of the moment) for months or even years to come.

Having a well-documented and well-understood crisis plan is also important even where the incident, and subsequent investigation, does not play out dramatically in real time. Investigations around corporate misconduct are an all too frequent example. It also pays to plan out these types of crises. For instance, and because discovery of corporate misconduct often has its genesis in internal investigations, companies typically have time to consider more fully how they will respond when the conduct eventually comes to light, and they should plan and test such scenarios. Even where there is less lead time – perhaps owing to a whistleblower's actions or a required corporate disclosure – there is inevitably some period for strategic preparation. In those moments smart companies turn to communications strategies that have been developed to be consistent with and to support their legal defences.

The 'disaster' scenarios are guaranteed to attract significant media attention and will require regular and active communications by a company. With other kinds of incidents that spawn investigations – such as those involving bribery and

corruption allegations, accusations of misconduct in the manufacturing supply chain, or accounting irregularities – it is often hard to predict at the outset the scale of the impact a company may be facing, making it all the more important to take action as early as possible to plan for different scenarios and to engage the right professional assistance. What may seem like an isolated incident likely to be a 'one-day story' could turn into something far worse if, for instance, deep-rooted company processes, historical conduct involving similar issues, the seniority of individuals involved or multi-jurisdictional problems are at stake.

Needless to say, the more systemic a problem appears to be, the more damage it is likely to cause to the company's reputation. Even minor incidents can become reputational nightmares if they raise questions about the integrity of internal systems, compliance and ethics, culture, or management's control of the organisation. As a result, the tempting choice for management – either to deny there is a problem or to rush to give public reassurance that a problem is limited to one or two individuals – can dramatically backfire.

Likewise, where an incident directly contravenes a company's public image or the reputation of its brand, the stakes are inevitably raised. Fraud, bribery and corruption allegations will be problematic for any company, but all the more so if the company has publicly made a virtue of its ethical conduct.

Large multinational organisations are also always going to be at a disadvantage when it comes to garnering the sympathy of the public, particularly where there are identifiable victims of alleged misconduct or negligence. So, being prepared to get ahead of issues early is a critical aspect of any company's reputational defence.

Ensuring close integration of legal and communications advisers 39.3

Planning for the fallout of a government investigation – whether that is done before the fact as part of crisis simulations or other preparation (which is preferable) or as the matter is unfolding (which is not ideal, but often the reality) – requires close collaboration between the company's lawyers and its communications advisers. Few companies have in-house communicators with backgrounds or expertise in complex legal issues. So, just as a company will turn to external counsel on major legal matters, it should turn to outside strategic communications advisers in similar circumstances.

The best-prepared clients understand the value of having a fully joined-up approach where the key speakers for a company (lawyers, communications professionals, investor relations teams, government and public affairs professionals) can coordinate regularly to ensure that every angle, stakeholder and perspective is covered. Working together, these individuals can also help ensure that messaging is consistent and disciplined with respect to all strategically important audiences.

The ideal way to proceed in these scenarios is to establish integrated teams that include in-house and external counsel and communications advisers who can work together in preserving or rebuilding reputation as the investigation unfolds. Without an integrated team, there is always the risk that communicators may be tempted to proceed without fully understanding the legal strategy, and lawyers will view the public communications concerns of a company as less important

than questions of legal liability and the eventual adjudication of the matter. These are problems that are only exacerbated where the situation is highly complex, fast-moving and public. Furthermore, without integration, the company's legal strategy may be forever undermined by inappropriate communications or the company's reputation may be lost for an extended period (perhaps even forever) if the company fails to communicate (or miscommunicates) during a crisis solely to preserve the legal arguments. For example, a lawyer not considering the communications aspects of a situation might advise a company to point to legal defences available to a corporation, such as intervening causes, contributory acts of a third party or negligence limited to low-level employees. While all might be valid (and eventually briefed and argued in court), thought should be given to how technical legal defences are heard by the public, by regulators, by investors and even by a company's employees. The goal should be to find ways to preserve the defences while communicating in ways that will be seen more positively by those stakeholders.

The benefits of synthesising communications and legal defence are legion. Communicators and others in regular contact with stakeholders can prove invaluable by providing the legal team with information, context and insights about how the investigation is perceived externally.

In addition to coordination, it is also indispensable to have in place sophisticated media monitoring tools throughout an investigation to track traditional media, social media and digital channels for any comments or interventions by investigating authorities, regulators, political voices and other relevant stakeholders. These include real-time reporting on news stories about the investigation and the company more broadly and monitoring or reporting on social media and blog discussions. Having alerts in place that go to all members of the integrated team to flag relevant developments for legal and public relations assessment is essential.

39.4 The key moments in any investigation

Having planned ahead and established the integrated team, the prudent company will need to prepare communications to manage external scrutiny and reputational impact on a number of occasions, but almost certainly at the following times:

- public disclosure of the investigation, whether that is initiated:
  - directly, by the prosecutor or investigator;
  - indirectly, through actions (such as a dawn raid, arrest or confiscation of evidence) that attract public attention;
  - by the company through legally mandated disclosures (such as in a securities filing) or otherwise; or
  - through a leak (deliberate or accidental) from any of the parties or individuals involved;
- high-profile comment on the progress of the investigation from interested stakeholders (media, analysts, investors, politicians, etc.);
- leaks of key documents or other information during the course of the investigation;

- the announcement of a settlement (or deferred prosecution agreement) and the initial response (which becomes an opportunity for the government to take centre stage);
- parliamentary or congressional hearings in parallel with an investigation;
- final decisions or judgments and the imposition of fines or other penalties; and
- court proceedings following an investigation.

In an ideal world, companies would have reasonable notice of any intention to launch an investigation, and particularly the intention of a regulatory body to comment publicly on proceedings. In practice, that often does not happen, especially where government investigators may perceive public relations benefits in making a surprise announcement.

In other situations, investigations will be launched in reaction to a media story, which means that the investigation, and more crucially the details of the allegations giving rise to it, will be public from the outset, and the affected company will necessarily find itself in a far more reactive mode.

If, by contrast, the company can self-disclose an issue or the existence of an investigation (particularly its own internal investigation), it will have an element of control over communications that is often absent where the government is making the decisions about announcements. Companies deciding to self-disclose may know the basic facts of the situation and have had time to work out the narrative to be presented in conjunction with the announcement. (In certain situations, it may even be possible to reach agreement on and coordinate such announcements with the authorities.) This period is a key window of opportunity for preparing the company's communications messages alongside ascertaining the company's legal position.

Another reputational issue to be considered is whether a company retains an independent investigator to conduct an inquiry into, for instance, ethical standards or compliance procedures, with the goal of having the independent investigator make remedial recommendations in advance of regulatory or prosecutorial authorities concluding their investigations. This step is not without its risks: many companies have found themselves in the position of making changes in the executive ranks because an independent investigator recommended it. But, in the appropriate circumstances, the appointment of an independent investigator can be extremely effective in helping position a company as seizing the initiative and communicating a sense that it is taking proactive steps to identify underlying problems while co-operating with an official external investigation. Should a company decide to proceed in this way, it will be an important moment to plan communications. Among other things (e.g., who to appoint and terms of reference), a company will have to consider whether it will agree to accept the recommendations of an independent agent, and whether it will agree to publish the resulting report, without reviewing them beforehand. In many cases, companies find that they have to do both. There is also the risk that if an investigator's report concludes with predominantly positive findings for the company, it will generate accusations of a whitewash despite the demonstrable independence of the investigator.

39.5 The impact of whistleblowers

Another issue that can have a significant impact on communications strategy is the presence of a whistleblower. Increasingly, whistleblowers go directly to a regulator or a media organisation to expose what they regard as improper conduct or other wrongdoing. In many cases, the company has no warning of the whistleblower's actions and may have had no opportunity to investigate the underlying charges, let alone devise a communications strategy. Moreover, given the disparity in stature of a corporation and a whistleblower, the strengthening of legal protection for whistleblowers in many jurisdictions and the media's tendency to give credence to whistleblower narratives, a corporation often finds itself at a disadvantage when responding to allegations of this sort: being seen to pick on the 'little guy' is never a winning reputational strategy.

Some take the view that, because many whistleblowers are disgruntled employees (or ex-employees), their motives are tainted. Others see whistleblowers as necessary and appropriate watchdogs to hold corporations accountable. Either way, companies must be very careful about deploying aggressive tactics to discredit them. Even where the whistleblower appears to be demonstrably compromised, a full frontal assault can backfire badly and introduce the perception that the corporation is a bully whose instinctive reaction is to lash out rather than accept the possibility that there has been a legitimate exposure of internal failures or wrongdoing by someone brave enough to speak out.

See Chapters 19 and 20 on whistleblowers

For all these reasons, the best (and often necessary) approach in most cases is for the company to respond to the sudden public emergence of a whistleblower with concern about the underlying allegations. The message must be put across clearly that the company is taking swift steps to investigate the allegations, that it takes seriously all allegations of the sort made by the whistleblower and that it has developed robust and effective procedures for dealing with concerns raised by employees.

39.6 Managing disclosures by regulators or prosecutors

Where an investigation is first made public by a government official such as a regulator, legislator or prosecutor, the company will have limited ability to influence the initial news cycle. The focus should turn immediately to trying to ensure that the subsequent reporting is balanced and fairly reflective of all relevant information. Of course corporations will also need to communicate with other stakeholders such as employees, business partners and shareholders through channels other than the media.

After disclosure of the investigation, a first question will be whether to react on the record. In most cases for companies, it makes sense to issue a holding statement – even if only to buy time. Telling the media that the company is reviewing the charges, allegations or statements and intends to co-operate with the investigation is not much, but it is better than making no comment because it conveys at least some action on the company's part. Depending on the coverage, that may be sufficient. Where the investigation is making a bigger splash, and particularly where it is proving unsettling to investors, staff and other key

stakeholders, a more substantive response is often necessary once a proper evaluation has been completed.

Public companies may also be under legally binding regulatory disclosure obligations requiring them to confirm otherwise confidential investigations in market announcements. These may be helpful in ensuring the market does not overreact and that the news (with its potential consequences) can be reflected in the share price early. On the other hand, even where more limited disclosures, such as in the legal matters section of regular results releases or the annual report, suffice from a legal point of view, these may not be enough to prepare investors and other stakeholders for the real scale of what may come. The lawyers, communicators and senior leadership of the company should evaluate the best course of action. In any event, the disclosures will need to be kept under constant review.

Where it is clear that the worst is yet to come, it is generally prudent to take the longer view and disclose as much of the information about potential ramifications for the company as rapidly as possible, but with carefully considered language that indicates the company is prepared for and in control of the situation. Although it may seem counterintuitive, presenting the worst-case scenario clearly and rationally can take a lot of the 'fear factor' out of market and wider stakeholder reaction.

The reason for this is simple: the media and other interested parties will want to piece together a narrative about the matter, filling in what they do not get from official sources with either their own or other people's speculation. Where it is possible to get the information out early, the company can effectively take the wind out of the sails of the speculation by preventing the drip-feed of details over an extended period, shortening the period of negative media focus. Of course this strategy, if pursued, must always be non-speculative and undertaken in close consultation with legal counsel to ensure that public statements are as narrowly circumscribed as possible to avoid potential damage to the company's legal defence and misleading information reaching the market.

As well as public statements 'on the record', an additional question is the extent to which the company or its communications advisers assist media with 'off-the-record' guidance or conversations 'on background'. These terms refer to the basis on which journalists are given information and are then able to use it. Constructive engagement of this sort with trusted journalists from mainstream media publications can be a useful and effective tool for conveying internally approved (non-privileged) contextual information and trying to ensure that prejudicial or inaccurate material does not make its way into reporting or, if it does, that it is corrected before it gains currency. Whether to engage, and the type of engagement appropriate in any given instance, will vary depending on a host of factors, including the particular jurisdiction.

All of this means that judging the right amount of information to disclose and on what basis is a delicate skill, and the best statements or announcements will always involve considered input from counsel, communicators and executives. This close coordination will help to avoid situations in which company representatives say or do things at an early stage that will look ill-judged in the light of subsequent events.

In addition, companies typically do well to avoid antagonistic or overly defensive reactions to criticism from regulators. Experience suggests that it is often better to be more circumspect, even if the company feels that criticism directed toward it is inflammatory, contentious or unfair. Snap reactions can lead to embarrassing climb-downs, especially when negotiated settlements may potentially be in the offing.

The best principle is to prepare for the worst while hoping for the best. Time spent preparing a toolkit of materials at an early stage will save time later on. If the company has prepared a crisis plan in advance – as discussed above – some of these materials will be readily to hand; others will be specific to the investigation and will typically include:

- process timelines (with trigger points for media and political interest);
- internal and external Q&As;
- script points for customer relations;
- draft statements;
- stakeholder maps (charting the state of engagement with or understanding of influential parties);
- leak strategies; and
- information on the company's contribution to key territories and its broader social purpose.

These materials can always be revised as the situation evolves and should form the basis for any content that the company needs or wants to publish about matters relevant to the investigation or its subject matter. Content is essential in corporate communications, especially given ever increasing demands for information in a fast-paced multimedia environment and the appetite for digitally accessible material. It is the communicators' job constantly to think creatively what materials may be needed for various purposes and for which particular channels, and to work with the legal advisers to ensure the messaging remains consistent with (and not a risk to) the company's legal position.

Legal counsel and communicators need to be sensitive to the complex dynamics in these situations, including the client's state of mind. Often the company's instinct is to push for robust public expressions of innocence and determination to fight the allegations. They may feel they are as much victims as anyone else in the drama, on the grounds of having been let down by subordinates or dragged into a situation they feel they could never be expected to have known about. Equally, too, they may find it hard to go along with the pragmatism of advisers who have more experience of managing these situations.

From a communications perspective, part of the pragmatism is understanding that there are no quick wins when an investigation is announced. It is the start of a potentially long process – a marathon not a sprint, with varied periods of intensity and activity. The company should be prepared for that and to dig in for a prolonged period.

Communications with stakeholders 39.7

It may seem obvious, but paying attention to stakeholders other than the government and media is critical during an investigation. These include senior management, non-executive board members, investors, industry analysts, other government agencies with which the corporation interacts or that regulate it, business partners, suppliers, lending banks, customers or clients, and staff. Investigations can consume large amounts of precious management time, but the business must continue, and be seen to continue, to function day-to-day. Maintaining morale and keeping problems in perspective are vital. Business-as-usual communications are something senior management neglects at its peril.

For that reason, even where there are restrictions on what can be communicated, particularly during negotiations to resolve a matter, it is important to have a properly developed and approved set of messages that can be used to ensure that interested parties have a basic understanding of the situation, and are clear that it is being handled properly and professionally. A well-crafted announcement for internal or select external audiences need not say all that much to pay dividends in creating support and a sense of inclusion at a difficult time.

Negative headlines and unhelpful speculation can adversely impact staff morale and unsettle clients or customers, particularly if certain products or sales practices are under investigation. Equally, there can be an opposite danger – that well-intentioned but misinformed parties feel they are doing the company a favour by weighing in, either through a public intervention or by leaking information without appreciating the implications of their actions. For both these reasons, proactive communications to affected or interested parties are worthwhile.

Whatever the type of communication, the essential touchstone is consistency of the message. While particular points may be emphasised more or less for each particular audience (what needs to be highlighted to investors may not be as relevant to clients or government contacts), there must be no contradictions or tensions in the core position of the company. This is again a key reason for coordination between lawyers and communicators: to ensure that the words used are approved for both internal and external use. Inconsistency in the messaging conveyed can cause real difficulty for companies, especially where a specific legal position has been agreed with investigating authorities and external communications are released that conflict with it.

Managing leaks 39.8

Although the substantive findings of investigations in virtually all jurisdictions are likely to be confidential until they have been concluded, leaks can occur for a variety of reasons. Generally, there is little in practical terms one can do to prevent them. In judging what, if any, strategy to deploy in response, it is again important to take a long view. It may not be ideal in the short term for a particular story to run; but coming out strongly against it may not help credibility and can store up problems for later when the company wants to be focused on rebuilding its reputation.

In any event, as set out above, having agreed adaptable leak strategies in place will be an important part of communications planning.

39.9 Role of third-party advocates

During investigations and related crises, third parties can often be helpful sources of commentary and information to articulate the company's point of view – especially where there is media appetite for commentators and 'talking heads'. Media and market analysts often need help understanding complex matters – both the substance and the process – and they frequently turn to industry experts, academics, former executives in the sector or even business partners. Communications professionals can be vital in developing these third-party sources and, in consultation with legal counsel, making sure they understand how to be helpful instead of harmful. In turn, those third parties can be invaluable in shaping coverage and external reaction, ensuring that the company's position is properly understood, and closing down unhelpful speculation before it gains currency and becomes established as 'fact'. In short, it is often useful to have a third party to steer media and other commentators to when it comes to reflecting or defending the company's position.

39.10 To fight or not to fight

At some point in every investigation or subsequent litigation comes the question whether to continue fighting or to settle. Companies, their lawyers and their communicators do not always see eye-to-eye on the right approach, and that will always depend on the circumstances. But companies would do well to understand the difference between what might get results in legal proceedings and what is convincing in the public arena. A perfectly valid legal strategy might actually alienate public opinion if, for instance, it sounds like an attempt to evade sanctions for serious moral or ethical failings by dint of a technicality. In those cases, litigating – even to victory – might do more long-term damage to the company's reputation than an early settlement would have. Which is not to say that the company should not fight – it should just think through the ramifications of doing so.

In some cases, it may be preferable from a reputational standpoint to acknowledge missteps and seek to resolve the matter early. Where this course includes a clear plan for dealing with any wrongdoers and a remediation plan, it can pre-empt the investigation's findings and help to draw a line under the issue. Often such a step can be beneficial in more ways than one, since plans like these are typically required when resolving a government investigation.

The concept of co-operation is obviously also a key element in handling investigations – from both a legal and a communications perspective. Companies may well assert that they have been and are being open, co-operative and transparent with investigators. But difficult issues can arise – especially in criminal investigations – when a company is either directly pressured to disclose material it considers is legally privileged or otherwise feels compelled to do so to demonstrate the extent of its co-operation with the investigation. Public tensions or arguments with investigating authorities about privilege tend to favour the authorities themselves because it is easier for them to create the impression that the company is being obstructive in refusing to give them the documents they have asked for than it is for the company to explain to the media and other parties why it believes

privilege obtains, why privilege matters as a fundamental right and why assumptions should not be made about a refusal to waive it.

The point may be academic in circumstances where, as happens more and more often in the United States at least, the government insists on a waiver in deferred prosecution agreements (DPAs) (which have more recently been introduced in the United Kingdom) or a criminal plea – although a waiver may not necessarily be a precondition of a DPA.

Ultimately a company will make this decision after careful deliberation based on all the circumstances, including the legal and financial implications of a refusal to waive and the possibility of prolonging or expanding the investigation. But where it feels that it has no real option, the release of privileged documents will then need to be considered in the context of communicating about the investigation.

The endgame: announcing a settlement 39.11

When it comes to positioning a company for announcement of the outcome of an investigation, several factors need to be considered. In the run-up to the announcement, the legal team needs to coordinate closely with communicators to make sure that any public statements are properly aligned with the agreed facts of the case. This is obviously paramount where companies have entered into DPAs with the authorities in which they are bound by prohibitions on making – or authorising lawyers, officers, directors, employees, agents or subsidiaries, etc., to make – any public statements contradicting the agreed statement of facts about the company's conduct. Procedures need to be in place to ensure that anyone speaking on behalf of the company – either in connection with the announcement or in other media or public stakeholder engagements (e.g., financial results presentations) – knows what it is permissible to say.

More broadly, so much of the approach to positioning an investigatory decision depends on the nature of the investigation, the sanctions or remedies imposed and the consequences for the particular company. Key questions will be:

- What are the core communications materials that the authority is itself planning to release or distribute on the day of announcement? Will it just be, for example, a press release with a copy of any relevant decision notices, rulings or agreements?
- How does the authority intend to choreograph it? Will there be a press conference and background briefings? Will the authority's leadership be giving news interviews for print and broadcast media?
- Where an investigation has involved more than one authority (domestically or cross-border), will the lead authority lead the communications? Are the authorities coordinating on communications?
- What is the range of sanctions against the company? Is it just a fine (which is likely to be the media focus)? Or are there other remedies – remedial compensation schemes, disgorgement of profits?
- How do the sanctions compare with other similar high-profile cases in size and scale?

- What are the potential consequences of the sanctions for the company?
- What are the other conditions attached?
- Is there a right of appeal?
- Are there likely to be satellite civil litigation proceedings or criminal prosecutions, perhaps against specific individuals?
- Will there be political reaction to the decision? If so, by whom?

Investigators, prosecutors and regulators know only too well that the opportunity to announce a big settlement against a corporation is their day. Their narrative will be taken to be the definitive account and will stand for official purposes as the public record. Seeking to contest that narrative where appeal is unavailable or unlikely is often not recommended (and may be forbidden), particularly as any attempt to contextualise, mitigate or otherwise play down the gravity of the misconduct is likely to backfire in reputational terms.

Nonetheless, a well-developed plan to position the settlement is a must for the company. A number of factors will need to be considered in the plan. In some cases, regulators will expect the company to issue statements expressing contrition, also perhaps setting out consequences for key individuals. This may entail resignations of senior management or board members. Even where this is not an express condition of a settlement, it is often the only credible response. Media and politicians may also expect there to be financial consequences for management who remain. Whatever the particular case, the company's statement will need to draw a line under the matter by conveying a concerted sense of moving forward. This can usually best be done as much out of the limelight as possible – press conferences or interviews with senior management, for example, can often force the company to go back over the very issues it is trying to put to bed.

Share price movement following an announcement will indicate how the market greets the result for public companies, and the impact may not necessarily be negative. The share price may even go up if shareholders broadly expected or are relieved at the result and welcome an end to the uncertainty of a prolonged investigatory process. But there may nonetheless be genuine questions that investors or other stakeholders will want answered. Given the size of some of the post-2008 settlements in the financial sector, investors have had legitimate questions about financial impacts and funding for the required payments.

In some cases, banks have had to announce capital raising measures to plug gaps left by fines. In these circumstances, companies need to have a clear plan in place for addressing all their key audiences, including (for public companies) capital markets through regulatory announcements. In addition, staff morale and relationships with certain customers may have taken a bad knock and may take concerted efforts by management over a long period to repair. Large customers and shareholders will need contacts at the right level of seniority. The roll-out plan will help to ensure that these conversations are properly sequenced to fit any public communications as well as internal briefings to both senior staff and line managers, who will in turn have to speak to key stakeholders.

Rebuilding reputation 39.12

Rebuilding a company's reputation actually starts the moment an investigation is first reported and continues throughout, including at the announcement of an outcome and beyond. Regardless of how the media perceives each of these points in the road, difficulties will arise if the company is seen to have failed to address or be addressing issues adequately. In such cases, other voices, such as politicians or investors, may start to wade into the conversation, raising the pressure on the company. In such situations, the only way to resolve the situation definitively may be to take steps that the company had hoped to avoid and to take them in circumstances where those measures will be seen to have been forced on the company.

Even if the headlines fade quickly, memories tend to linger. Companies care about their brands and reputations, so they will need to devote significant time, thought and energy to repairing damaged relationships and restoring trust. In many cases, the remediation plan will require difficult actions or statements that convey genuine remorse and a desire to change on a cultural level, and potentially some more practical measures to repair specific failings in procedures and controls. The goal will be to move the company from being seen as part of a wider problem and position it as a proactive part of the solution.

To achieve that outcome will require an honest appraisal of the mistakes and a determination to do what is necessary to rectify them. Serious polling and data-driven analysis will help identify where exactly the reputational damage lies and also help track success in tackling those issues and clawing back trust. Crucial and often forgotten is the need for extra vigilance to ensure that the company avoids committing further errors. In the recovery period, even the slightest issue risks being blown up and setting the company even further back. It is important, too, that the chief executive owns the reputation recovery plan and that he or she and everyone else involved understands that actions really do speak louder than words.

Summary: 10 key considerations 39.13

In summary, and drawing on the above, the following is a practical checklist of communications considerations to bear in mind when navigating an external investigation:

1 *Context*: Understand the company's backstory and track record, as well as any political agenda of the investigating entity.
2 *Planning*: Undertake as much advance planning as possible, preferably through crisis exercises, and preparation and planning.
3 *Integrated teams*: Put together a core integrated team to ensure that the legal advisers are plugged into the communications function and other key functions (e.g., investor relations, public affairs).
4 *Active monitoring*: Have in place monitoring tools to track continuously for media coverage, both traditional and on social media channels. Information about who is commenting on the process or wider debate, influencing opinion and affecting the climate, is essential.

5 *Core content*: Content is king. Put together a core suite of materials that can be continuously updated as events change – process timelines, key messages, Q&As, holding statements, stakeholder lists and general information about the company's contribution to key territories and overseas markets. Consider creating public-facing content that can be accessed or distributed digitally via the company's communications channels.
6 *Consistency of message*: Ensure there's consistency of messaging – jointly developed by the legal and communications teams (with input from other functions) – around key moments in the investigation, especially the final outcome.
7 *Stakeholder management*: Consider what the company's most immediate key audiences (beyond the media) understand about the investigation and its implications for them, and what the company can say to keep them informed: senior management, non-executive board members, investors, industry analysts, other government agencies with which the corporation interacts or that regulate it, business partners, suppliers, banks, customers or clients, and staff.
8 *Third-party advocates*: Identify third parties who can potentially provide helpful comment about the process or about the company more generally: industry analysts, former executives in the industry and business partners. Equally, know the company's enemies and who might weigh in against the company's interests.
9 *Business as usual*: Convey a clear sense that the company is in control of the investigation and that the leadership is focused on the process of getting on with day-to-day business.
10 *Reputational rebuild*: Consider throughout the investigation what the company may need to do to communicate genuine cultural or behavioural change, using the investigation outcome as a pivot point for building the company's reputation.

40

Data Protection in Investigations

Stuart Alford QC, Serrin A Turner, Gail E Crawford, Hayley Pizzey, Mair Williams and Max G Mazzelli[1]

Introduction 40.1

Data protection law is a misleading term because the relevant framework will be a combination of employment, whistleblower, criminal and privacy laws. Companies and practitioners must navigate domestic and international legislation that touches on data protection, while ensuring they stay on the right side of regulatory and prosecuting agencies and co-operate with them to the extent that it is of benefit.

Handling data about individuals has become increasingly complex, particularly where the data protection regimes in different jurisdictions appear to be imposing conflicting obligations on data holders.

This chapter will look at both UK (including some European) and US laws and how they frame issues around investigations and data protection. We will look at internal investigations and those conducted by authorities, and provide some specific guidance in respect of data protection and whistleblowing regimes.

In the United Kingdom, a balance must be struck between a company's compliance and regulatory obligations that require the processing of data as part of investigations, and the protection afforded to individuals caught up in those investigations, primarily under the European General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 (DPA 2018). UK laws governing the interception and monitoring of communications may also require navigation in the context of internal investigations. Although legislation protecting individuals' data has existed for years, the increased sanctions for breaches under the GDPR (maximum fines being the higher of €20 million or up to 4 per cent of annual

1 Stuart Alford QC, Serrin A Turner and Gail E Crawford are partners and Hayley Pizzey, Mair Williams and Max G Mazzelli are associates at Latham & Watkins.

worldwide turnover), and increased regulator focus on data privacy, means that those conducting investigations must take the protections afforded to individuals more seriously than they did previously. The GDPR (which took effect on 25 May 2018) largely consolidated the previous European data protection regime and sought to harmonise the position within the European Union, but it does not necessarily simplify the issue between Member States. Each Member State may have its own laws in place as long as the basic standards of the GDPR are met; the GDPR is a floor and not a ceiling.

Furthermore, the GDPR not only catches EU corporations and global company groups with an EU presence (including their use of personal data outside the European Union to the extent that use is intrinsically linked with their EU activities), but also affects any corporations outside the European Union and with no EU presence that actively offer goods and services to, or monitor the behaviour of, individuals within the European Union, even if the data is stored outside it.

In the United States, there is no uniform, omnibus federal privacy regime comparable to the GDPR. However, a patchwork of federal and state privacy laws may come into play in an internal investigation, particularly in the context of reviewing and collecting employees' electronic communications. To minimise legal risk, companies should provide employees with clear notice that their electronic communications stored on company systems or devices are subject to monitoring and search.

Given the GDPR's extraterritorial reach, US and multinational companies may have to grapple with GDPR compliance obligations in conducting an internal investigation or responding to criminal or regulatory investigations. Where a US or multinational company's obligations to comply with US legal demands for personal data conflict with the GDPR's limits on the processing and transfer of that data to the United States, the company must assess whether it can lawfully transfer responsive data to the United States that is subject to the GDPR. If not, the US or multinational company may need to negotiate with the requesting legal authority to narrow the scope of the request or to develop other ways of resolving the legal conflict. Where the conflict cannot be resolved, the US or multinational company may need to consider challenging the request on comity grounds, although such challenges have rarely succeeded in the context of criminal or regulatory investigations.

40.2 Internal investigations: UK perspective

Internal investigations will inevitably deal with personal data, particularly employees' data, and in the United Kingdom this is governed by the GDPR and DPA 2018. For those conducting internal investigations, the key obligations to consider are (1) transparency, namely the requirement to inform individuals about how their personal data is being used (unless there is a relevant exemption), (2) data minimisation, namely the requirement to ensure that use of personal data for the investigation is proportionate, (3) establishing a legal basis for the processing of personal data, as prescribed by the GDPR (consent and legitimate interest are two of the legal bases companies and practitioners can commonly rely on to

process data in an internal investigation), (4) if relevant, establishing a relevant condition on which to process any 'special categories' of personal data or any criminal offences data involved (in addition to a legal basis for the processing), and (5) if personal data will be transferred, or accessed from, outside the European Union, ensuring a legal basis for that data transfer, as prescribed by the GDPR (in addition to a legal basis for the underlying processing).

Transparency 40.2.1

The GDPR and DPA 2018 require relevant organisations to inform individuals in advance about how their personal data is processed, in a clear and accessible manner, and prescribe the minimum information to be provided.[2] This forms part of the wider GDPR principles of transparency and fairness, which seek to prevent organisations from using data in ways that are detrimental, unexpected or misleading to individuals. Meeting these obligations in the context of internal investigations can present practical challenges if an organisation does not have a comprehensive monitoring policy, as use of employees' personal data for investigation purposes may well be detrimental to, and unexpected by, those employees.

There are certain exemptions under the DPA 2018 to the specific obligation to provide minimum information to individuals. (The exemptions do not apply to the requirements to process personal data transparently and fairly.) When collecting personal data directly from an individual, organisations are not required to provide data protection information that the individual already has. This may be relevant for organisations conducting investigations into, or involving, their employees and using personal data the organisation has obtained from them, if the organisation already provides some level of privacy information to them. A wider range of exemptions are available in circumstances where the personal data is obtained from other sources. The most relevant in the context of internal investigations apply if providing the information to the individual would be impossible or would involve disproportionate effort; providing the information to the individual would render impossible or seriously impair achievement of the objectives of the processing; or the organisation is required by law to obtain or disclose the personal data (which necessitates a binding legal obligation, rather than, for example, compliance with a non-binding code of practice or an informal, non-binding regulator request).

In addition to the transparency principles under the GDPR, the UK's regulatory framework for communications monitoring also requires organisations to be transparent with employees about the interception and monitoring of their communications (both in written policies and also in consistent business practices). Taken together in the context of internal investigations, the data protection and communications regimes oblige organisations to be clear and open with employees about how their personal data and their communications are used, and to

2 This minimum information includes, among other things, the purposes of the processing, the lawful basis for the processing, the recipients or categories of recipients of the personal data, details of data transfers outside the EU and applicable data retention periods.

ensure that any interception and subsequent review, use and disclosure of data and communications in an investigation is both lawful and proportionate. Robust, clear and accessible data privacy information notices for employees, as well as policies on employee monitoring, will provide a valuable shield against claims of employee privacy infringement and non-compliant monitoring practices – at least in the United Kingdom.[3]

40.2.2 Data minimisation

The GDPR principle of data minimisation should be applied by organisations across their personal data activities generally, including internal (and external) investigations. Organisations should ensure that the collation, review, use and disclosure of individuals' data during the investigation is proportionate and no more intrusive than is necessary to achieve the legitimate purposes of the investigation. This will be relatively straightforward for clearly defined and focused investigations, but may prove more challenging to assess in practice in wide-ranging investigations requiring significant levels of data for loosely defined purposes. Organisations would be well advised to document the investigation's scope and associated personal data proportionality assessment, to demonstrate that data minimisation principles have been applied. Practical safeguards to ensure proportionality should also be applied, such as appropriately limiting the scope of documentation, email and communications review and disclosure (limiting impacted custodians and individuals, using key word searches and time periods to identify relevant information, etc.).

40.2.3 Legal basis for data processing: consent

Consent from the individual provides a legal basis for the processing of that individual's personal data, provided the GDPR consent conditions are met. The GDPR establishes a higher standard for consent for the processing of personal data than the Data Protection Act 1998 (DPA) it replaced.[4] Consent must be given clearly and in plain language and must be an affirmative act – consent cannot be given by inactivity, such as pre-ticked boxes in an online form.

In the typical employer–employee context of an internal investigation, the concept of consent being freely given is a complicated one. Given the dynamic, some jurisdictions consider that consent from an employee to an employer may never be freely given, a position exacerbated in an internal investigation by the added element of potential wrongdoing by the employee or another individual, and tipping-off considerations. Investigators should ensure they comply with the GDPR, either by getting express consent from the data subject to process their data, which may not be feasible in an internal investigation if it cannot be

3 The position in a number of other European jurisdictions (including France and Germany) is considerably more protective of employee rights and restrictive of an employer's ability to intercept or review communications or to access employee devices.

4 GDPR, Article 7 and Recital 32.

considered freely given or because the organisation does not want to notify the individual of the investigation (blanket clauses in employment contracts will no longer be enough), or by relying on one of the other lawful bases under the GDPR (discussed below) to lawfully process the data.

Legal basis for data processing: legitimate interest 40.2.4

The GDPR provides a number of other legal bases for the processing of personal data in certain circumstances.

Under the GDPR, an organisation can consider the legitimate interests of a third party or public interest, as well as its own legitimate interests, when assessing the use and processing of personal data.[5]

In an internal investigation, this ability could allow an organisation to rely on the lawful basis of legitimate interests (of a third party or public interest) to process personal data. The rights of individuals can, however, override a legitimate interest, if the effect on an individual's interests or fundamental rights override the organisation's (or a third party's) legitimate interests.

The UK's Information Commissioner's Office (ICO) enforces data protection legislation and has stated: 'Legitimate interests is the most flexible lawful basis for processing.' The ICO has set out a three-part, cumulative test for establishing whether there is a legitimate interest in processing the data, which may be a useful addition to an investigation plan:

- Purpose test: is the purpose of the processing a legitimate interest?
- Necessity test: is the processing of the data necessary and proportionate for the purpose?
- Balancing test: is the legitimate interest overridden by the individual's interests?[6]

The above test can be used by those conducting internal investigations to justify the processing of data under the GDPR because it is for the legitimate purpose of the company itself, or a third party, provided any risk of undue harm to the individual does not outweigh that interest. In respect of the necessity test, companies must consider whether there is an alternative, less intrusive, means of gathering or processing the same information.

To demonstrate compliance with the GDPR, organisations will have to document their decisions carefully (through a legitimate interests assessment).[7]

5 This provides additional flexibility to data processors; under the Data Protection Act 1998 (DPA), third-party interests were restricted to those third parties to whom the data would be disclosed.

6 'Legitimate interests' (Information Commissioner's Office): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

7 Ibid.

40.2.5 Special category and criminal offences data

When processing data in an internal investigation, data controllers must pay increased attention when dealing with special category data[8] (which replaces the 'sensitive personal data' terminology under the DPA, and expands the categories of personal data subject to additional restrictions). In an internal investigation, this kind of information will often be held in a human-resources file that becomes part of a review within the investigation. There is a possible question mark over whether employee emails or instant messages, etc., could be considered special category data, as they could potentially contain data within this definition. This is not clear, however, and it is certainly arguable that emails should not fall into this category on the basis that any special category data is incidental and not part of the primary purpose of the use of data in that context. This argument is strengthened by the application of data minimisation steps to ensure the special category data is not specifically identified or targeted as part of the investigation. The concept of special category data is dealt with under Article 9 of the GDPR (and section 10 of the DPA 2018) and it has been extended to include genetic and biometric data.

When dealing with special category data, organisations must establish both a legal basis for the data processing (e.g., consent, legitimate interests or another basis under the GDPR) and an additional, specific legal basis for processing the relevant special category data. The GDPR and DPA 2018 provide for a number of specific legal bases or conditions for the use of special category data, the most relevant of which for internal investigations are consent of the individual (specifically to the use of his or her special category data), processing for the purposes of establishing or defending a legal claim, and public interest purposes as specifically provided for in national law.

Information about criminal allegations, proceedings or convictions in relation to an individual may also be relevant in the context of an internal investigation. This data is treated separately under the GDPR, and requires a lawful basis for processing and legal or official authority to handle that data, which must be specifically prescribed under national law. In the United Kingdom, the DPA 2018 authorises the processing of criminal offences data in certain limited circumstances and subject to the conditions set out in the DPA.[9] These legal authority grounds are narrow, though certain grounds may be available in internal investigations, including prescribed public interests grounds, consent of the individual and establishing or defending a legal claim. Special category data and criminal convictions data should be handled with particular consideration, and organisations should ensure that the basis on which they are using this data is clearly documented.

8 Special category data is defined in the GDPR and the DPA 2018 as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation' (Article 9 of the GDPR and section 10 of the DPA 2018).

9 DPA 2018, Part 1 and Schedule 1.

Public interest 40.2.6

The public interest ground for processing special category or criminal offences data may be useful in an internal investigation, especially where it is likely to be followed by a regulatory investigation, and where consent or another legal basis is not available in practice. However, this ground is limited to those public interest purposes that are specifically provided for in national law. Under the DPA 2018, these public interest purposes are relatively narrowly defined, meaning this ground will be difficult to satisfy in practice, and organisations should be confident in, and have clearly documented, their justifications before relying on this basis.

Under the DPA 2018, the public interest purposes of particular relevance to internal investigations relate to the prevention or detection of unlawful acts, and to protecting the public against dishonesty, in both cases provided there is also a 'substantial public interest'.[10] Both provisions require that processing be done without consent of the individual, to avoid prejudicing the investigation. The scope of the public interest ground for data processing under the GDPR must be provided for under national law, and may vary across the European Union. Organisations should therefore seek local legal advice in the relevant Member States.

Data transfer outside the European Economic Area 40.2.7

Given the international scope of many investigations, companies should consider the practicalities of exporting data while complying with the GDPR. If the personal data will be transferred, or accessed from, outside the European Economic Area (EEA) – whether from within the organisation's corporate group or externally – that data transfer also requires a separate lawful basis under the GDPR, in addition to the lawful processing of the data itself. This restriction on data transfers does not apply to non-EEA countries recognised as 'adequate' by the European Commission, to which personal data may be transferred freely.[11] Investigations involving data transfers to countries or entities outside the EEA and not recognised as 'adequate' will require other grounds or safeguards to enable the transfer, as set out in the GDPR. The safeguard most commonly relied on in this context, for intra-group transfers within an organisation or to or from third-party providers involved in the investigation, consists of using standard contractual clauses (SCCs).[12] These are European Commission approved standard-form contractual agreements that put in place binding data protection obligations between the data exporting and data importing entities.[13] Many international organisations are likely to be familiar with the SCCs as part of their wider data privacy

10 Ibid., at Schedule 1, Part 2.

11 Currently, Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, Uruguay and United States (for Privacy Shield certified organisations only), are recognised as having adequate protection. Adequacy talks with South Korea are ongoing.

12 Sometimes referred to as the 'Model Clauses'.

13 The current versions of the standard contractual clauses can be accessed at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

compliance efforts. There are alternatives to the SCCs under the GDPR, though they may not be as reliable in practice for organisations conducting investigations. This includes the explicit consent of the individuals, and transfers required to establish or defend a legal claim (applicable for occasional transfers only).

In the event of a no-deal Brexit, the GDPR rules on data transfers will be mirrored into UK law, therefore personal data transfers from the United Kingdom will be subject to similar restrictions and requirements, except in relation to transfers to EEA Member States, which can continue unrestricted.[14] The requirements for data transfers from the United Kingdom to countries outside the EEA will remain similar to current GDPR rules, and the UK government has confirmed that it intends to recognise existing EU adequacy decisions and approved SCCs wherever possible. In relation to transfers from the EEA to the United Kingdom, following any no-deal Brexit when the United Kingdom will cease to be an EEA state, the GDPR's data transfer rules will apply to restrict those data transfers. The UK government has indicated its intention to apply for an adequacy decision from the European Commission in these circumstances (therefore allowing personal data to be transferred freely from the EEA to the United Kingdom), though that will inevitably take time to be negotiated, and granted and the outcome is not currently clear.

Different data transfer considerations apply in the context of investigations by authorities.

40.2.8 Third parties to investigations

Companies and practitioners often rely on third parties to assist with internal investigations (for example in data analysis, legal advice or document review). These third parties will very often require access to personal data in order to act. The GDPR has introduced new requirements when entering into such arrangements, which means that a contract or other legal act under European Union or Member State law is now required where controllers engage the services of processors.

This must set out, among other information, the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller, as well as certain prescribed contractual obligations.[15] The GDPR changed the required clauses, so it is particularly important to ensure that the correct agreements are in place from the outset of any interaction with third parties. In addition, any agreement must contain an obligation of confidentiality.[16]

14 UK Department for Digital, Culture, Media & Sport Guidance on 'Amendments to UK data protection law in the event the UK leaves the EU without a deal', 23 April 2019.

15 GDPR, Article 28(3).

16 Ibid., at Article 28(3)(a) to (h).

Monitoring employees' electronic communications 40.2.9

In addition to the data protection considerations discussed above, a framework of regulations is in place in the United Kingdom to govern the extent to which employers can intercept and monitor their employees' electronic communications.[17] These communications regulations are triggered on 'interception' of communications, defined as making the content of the communication available to a person who is not the sender or intended recipient, whether before, during or after transmission of the communication. In the context of internal investigations, this will most likely be of relevance when considering investigation-specific interception and monitoring of employee communications, or when assessing the legality of an organisation's existing communications monitoring practices.

The default position is that employers may not intercept employee communications other than with the consent of both the sender and the recipient of the communication, or as authorised by the exemptions built into the legal framework. In practice, organisations carrying out internal investigations are most likely to rely on exemptions that permit interception: to monitor employee or external users' compliance with rules governing use of the system (whether internal policies or legal or regulatory requirements); to maintain records and establish facts; to prevent or detect crime; or for information security purposes.[18] If consent is relied on for interception purposes, this should be distinguishable from any consent relied on for GDPR purposes (which sets a higher consent standard), so that both interception and data protection consents can be evidenced if required.

Internal investigations: US perspective 40.3

The United States has no single unified data protection regime. However, a patchwork of federal and state privacy laws impose various constraints on the extent to which a company may collect and review information about its employees, particularly their electronic communications.

State privacy laws in the United States vary considerably, but many states recognise a common-law right against unreasonable intrusions into a person's seclusion or privacy. Such causes of action have been brought against employers in the context of searches in the workplace.[19] While courts have typically upheld an employer's right to search company-owned property, including computers

17 This framework consists primarily of the Regulation of Investigatory Powers Act 2000 (RIPA); the Investigatory Powers Act 2016 (IPA 2016), which updates and repeals certain parts of RIPA; the Interception of Communications Code of Practice under the IPA 2016; and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Lawful Business Practice Regulations), which were enacted under RIPA but have not to date been replaced or repealed by the IPA 2016.

18 Provided for under the Lawful Business Practice Regulations and the Communications Code of Practice.

19 See, e.g., *Rowe v. Guardian Auto. Prods.*, 2005 WL 3299766 (N.D. Ohio 6 December 2005); Restatement (Third) of Emp't Law: Emp't Privacy & Autonomy ch. 7 (Council Draft No. 6, 2011), available at http://extranet.ali.org/docs/Employment_Law_CD6_online.pdf (introducing the tort of wrongful employer intrusion upon a protected employee privacy interest and stating

and devices, there is no bright-line rule. In cases involving more unusual facts, an employee may be able to make out an invasion of privacy claim based on a workplace search.[20] Accordingly, companies are well advised to have written policies, that all employees must acknowledge, clearly providing that the company's network and systems are subject to monitoring and search. An employee will face difficulty establishing a right to privacy in company-controlled systems or data where such policies are in place.[21]

Other state laws place more specific prohibitions on employers that can limit the outer bounds of a company's investigative actions. For example, various state laws prohibit questioning an employee on issues that serve no business purpose,[22] demanding an employee disclose passwords and other credentials to his or her personal email and social networking accounts,[23] requiring employees to alter privacy

---

that '[e]mployees have a right of privacy against wrongful employer intrusions upon protected employee privacy interests' including personal information).

20 See, e.g., *Doe v. Kohn Nast & Graf*, 866 F. Supp. 190 (E.D. Pa. 1994) (allowing an invasion of privacy case to proceed to jury based on a company's opening of mail sent to the workplace that appeared to be personal in nature); *Rene v. G.F. Fishers, Inc.*, 817 F. Supp.2d 1090 (S.D. Ind. 2011) (allowing claims under the Stored Communications Act (SCA) and the Indiana Wiretap Act to survive where a company decoded the employee's passwords to personal accounts which had been accessed on company computers).

21 See, e.g., *Leventhal v. Knapek*, 266 F.3d 64 (4th Cir. 2000) (finding no legitimate expectation of privacy in internet use when an employer's known policy allowed monitoring of 'all file transfers, all websites visited, and all e-mail messages'); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (holding that employees did not have an 'objectively reasonable expectation of privacy' in email messages stored on computer network); *Garrity v. John Hancock Mut. Life Ins. Co*., 2002 U.S. Dist. LEXIS 8343, at *5 to 6 (D. Mass. 7 May 2002) (that an employer instructed its employees on creating personal passwords for their computers did not create reasonable expectation in privacy); *Muick v. Glenayre Elecs*., 280 F.3d 741 (7th Cir. 2002) (employee did not have reasonable expectation of privacy in his company-owned laptop); *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. 15 September 2004) (employee had no reasonable expectation of privacy in websites accessed on work computer where company had a policy regarding personal computer use and monitoring); *Garrity v. John Hancock Mutual Life Insurance Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. 7 May 2002) (the employee had no reasonable expectation of privacy in emails transmitted on an employer's computer system where the employer's interest in preventing sexual harassment was greater than the employee's privacy interest); Restatement (Third) of Emp't Law § 7.03 (Council Draft No. 6, 2011). ('[A] clear employer notice or policy that a particular location is not private for employees generally defeats an employee's expectation of privacy, unless the employer's actual practices contravene the wording of an express notice or policy.'); *O'Connor v. Ortega*, 480 U.S. 709, 713 (1987) (plurality opinion) (stating that a government employee had a reasonable expectation of privacy in his desk and file cabinets where 'there was no policy of inventorying the offices of those on administrative leave' and 'there was no evidence that the Hospital had established any reasonable regulation or policy discouraging employees such as Dr Ortega from storing personal papers and effects in their desks or file cabinets').

22 See 2 Cal. Code Regs. § 7286.7(b) (prohibits employers from inquiring into any issues that otherwise serve no 'business purpose').

23 See, e.g., Cal. Labor Code § 980.

settings on their electronic accounts,[24] or asking employees to access social media accounts in the presence of the employer.[25]

Various state and federal laws also restrict the collection of electronic communications, including emails[26] (both work and personal), phone calls[27] and social media accounts.[28] One primary federal law is the Electronic Communications Privacy Act,[29] which breaks down into the Wiretap Act (which generally prohibits intercepting electronic communications),[30] the Pen Register Statute (which generally prohibits use of a pen register to track communications)[31] and the Stored Communications Act (which generally prohibits unauthorised access to stored electronic communications).[32] These statutes do not generally prohibit an

24 See, e.g., 26 M.R.S.A. § 615.

25 Id.; see, e.g., Cal. Lab. Code § 980 (2012) (allowing an employer to require an employee to 'divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations,' but information must be used solely for the investigation); 820 Ill. Comp. Stat § 55/10 (2012) (granting an employer the ability to require employees to share specific content of personal online accounts (but not user name and passwords) that has been reported to the employer for purposes of investigating employee misconduct); Wash. Rev. Code § 49.44.200 (2013) (permitting an employer to require an employee to share content (but not the login information) from his or her social media account as necessary to comply with applicable laws or investigate employee misconduct).

26 See *Scott v. Beth Israel Med. Ctr., Inc.,* 17 Misc. 3d 934 (Sup. Ct. N.Y. Cty. 2007) (holding that a policy that employees had no privacy right over material created, received, saved, or sent using the employer's computer system sufficient to eliminate any expectation of privacy); *United States v. Etkin*, 2008 U.S. Dist. LEXIS 12834, at *14 to 16 (S.D.N.Y. 20 February 2008) (employees do not have a reasonable expectation of privacy when employers warn the employees via log-on notices or flash-screen warnings of a policy through which the employer could monitor or inspect the computers at any time); *United States v. Angevine*, 281 F.3d 1130, 1135 (10th Cir. 2002) (holding no reasonable expectation of privacy where an employer's policy 'clearly warned computer users [that] data [wa]s "fairly easy to access by third parties"'); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (holding that any reasonable expectation of privacy employee had in his work computer was eliminated when the employer announced that it could inspect the computer).

27 Some states require the consent of all parties to legally record a phone call. See, e.g., Cal. Penal Code § 630 et seq. (2006); Conn. Gen. Stat. § 52-570d (2006); Fla. Stat. §§ 934.01 to .03 (2005); 720 Ill. Comp. Stat. 5/14-1, -2 (2006); Md. Code Ann. Cts. & Jud. Proc. § 10-402 (2006); Mass. Gen. Laws ch. 272, § 99 (2006); Mont. Code Ann. 45-8-213; N.H. Rev Stat. Ann. §§ 570-A:l, -A:2 (2005), as amended by New Hampshire Laws Ch. 169 (H.B. 1353) (2016); 18 Pa. Cons. Stat. § 5701 et seq. (2005); Wash. Rev. Code § 9.73.030 (2006). Other states require just one party consent. See, e.g., Ariz. Rev. Stat. Ann. § 13-3005; D.C. Code Ann. § 23-542(b)(3); N.Y. Penal Law § 250.00(1); N.J. Rev. Stat. § 2A:156A-4(d); Ohio Rev. Code Ann. § 2933.52(B)(4); Tex. Penal Code Ann. § 16.D2(c)(4).

28 See, e.g., Cal. Lab. Code § 980; 19 Del. Code § 709A(b); Md. Code Lab. & Empl. § 3-712(b)(1); Nev. Rev. Stat. § 613.135; N.H. Rev. Stat. § 275:74; 820 Ill. Comp. Stat. § 55/10(b)(1).

29 See 18 U.S.C. §§ 2510-22, 2701-12.

30 Id., at §§ 2511-2522.

31 Id., at §§ 3121-3127.

32 Id., at §§ 2701-2711.

employer from searching its own email system.[33] However, they may limit an employer's ability to use company-owned equipment to access an employee's communications stored with third-party providers (e.g., Gmail),[34] at least without the employee's consent.

Other state laws govern an employer's ability to collect and use biometric data like fingerprints, voice prints or vein patterns from employees. One such law is the Illinois Biometric Information Privacy Act (BIPA).[35] BIPA defines biometric information broadly to include 'any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual'.[36] Employers who intend to use such biometric information for any purpose, including for time management, security access or safety, must first obtain informed written consent prior to collection.[37] Employers can obtain consent via an employment agreement.[38] A failure to obtain proper consent, among other things,[39] can result in potential exposure to liability,[40] as the Illinois Supreme Court has ruled that any violation of the law – regardless of the presence of particularised harm – confers standing on the affected individual to sue for potentially substantial statutory damages.[41]

Finally, besides state and federal laws, internal investigations in the United States may also be subject to the GDPR's restrictions, given its extraterritorial reach. In particular, to the extent the investigation requires review of personal data stored in the European Union – for example, an employment file for an employee in an EU affiliate, stored on a server in the European Union – then the company must evaluate whether (1) the EU company has a legal basis on which to disclose the data to the United States, (2) transparency obligations have been met and relevant information or notices have been provided (or an exemption applies), (3) data minimisation and proportionality principles have been applied and (4) one of the conditions for the transfer of personal data to the United States

33 Id., at § 2701; see, e.g., *Fraser v. Nationwide Mut. Ins. Co*., 352 F.3d 107 (3d Cir. 2003) (holding that the insurance company that leased a computer system to an agent did not violate the Electronic Communications Privacy Act (ECPA) when it retrieved stored emails from computers).

34 See 18 U.S.C. § 2701(a); see, e.g., *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 757, 758 (N.D. Ohio 2013) (denying an employer's motion to dismiss claims under the ECPA where an employee alleged that her supervisor accessed unopened emails from her Gmail account through her employer-issued BlackBerry).

35 740 ILCS 14/1 (2008).

36 Id., at § 10.

37 Id., at § 15.

38 Id., at § 10 ('"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.')

39 BIPA also regulates the disclosure, protection and retention of, as well as profiting off of, biometric information by employers. See id., at § 15.

40 Id., at § 20 (BIPA provides for a privacy right of action).

41 See *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 34 (Ill. 2019) ('When a private entity fails to adhere to the statutory procedures . . . the right of the individual to maintain his or her biometric privacy vanishes into thin air. . . . The injury is real and significant.' (internal quotations and modifications omitted)).

has been met. If the organisation cannot meet the above requirement to legitimise the transfer, the company may wish to consider ways of handling the data that do not involve transferring personal data to the United States – such as reviewing the relevant personal data in the European Union, or redacting personal information from the data set before it is transferred.

Investigations by authorities: UK perspective 40.4

Companies have always had to consider competing interests when dealing with investigating authorities, but until now data protection has rarely been near the top of any list of considerations. The very significant fines available under the GDPR mean that companies must take data protection much more seriously, particularly the handling of personal data to authorities both in the United Kingdom and overseas. The ICO has shown that it will not hesitate to use its powers under the GDPR to investigate and issue significant fines for breaches. For example, on 8 July 2019, the ICO announced a notice of intent to fine British Airways £183.39 million[42] for a data breach affecting 500,000 individuals brought about by 'poor security arrangements'.[43] This was closely followed by a further notice of intent to fine on 9 July 2019 whereby the ICO is proposing to fine Marriott International £99.2 million[44] for infringements of the GDPR stemming from a data breach at Starwood, which Marriott acquired in 2016, effecting 300 million individuals.[45] It remains to be seen whether this initially robust approach to GDPR enforcement from the ICO will extend into the more nuanced environment of internal and regulatory investigations, with their frequently competing legal obligations.

Guidance from authorities 40.4.1

Prior to the introduction of the GDPR, concerns were raised about the balance companies should strike between their reporting and regulatory commitments (including investigations), on the one hand, and protecting their employees' (or anyone else's) personal data on the other. To offer some guidance in this regard, the Financial Conduct Authority (FCA) and ICO published a joint update on the GDPR in which they made clear that they believed 'the GDPR does not impose requirements which are incompatible with the rules in the FCA Handbook'.[46] Further, the FCA and ICO have published a memorandum of understanding,[47] which (among other things) pledges each regulator to seek to understand and,

42 1.5 per cent of British Airways 2017 global revenue and the largest proposed fine under the GDPR to date.

43 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

44 2.5 per cent of Marriott's 2017 global revenue.

45 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

46 https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr.

47 https://ico.org.uk/media/2614342/financial-conduct-authority-ico-mou.pdf.

where appropriate, collaborate and co-ordinate work on their respective policies that have a material effect on the other's objectives. This is yet to be tested and it is unclear whether the FCA will be tolerant of delays, limitations on information and other issues caused by a company's cautious approach to data protection.

Furthermore, the FCA has been keen to point out that it will be considering breaches of the GDPR as part of its supervision of senior management arrangements, systems and controls.[48] Although this is limited to entities regulated by the FCA, it seems likely that other authorities will take a similar approach and companies will need to be ready to show that they have taken their data protection obligations – ongoing and as part of an investigation or data request from a investigating authority – seriously.

40.4.2 Providing data to authorities

Where authorities make requests for data, companies must be absolutely clear about the legal powers by which those requests are being made, to ensure that they can comply with the request while fulfilling their GDPR obligations. The benefits of voluntarily handing over more data than specifically required have probably disappeared with the GDPR's tougher data regulation regime. Among other things, the GDPR requires organisations to be transparent and provide information to individuals, to minimise use of personal data, to establish a legal basis for processing personal data and to legitimise any transfers of data outside the EEA. These obligations apply equally in the context of data disclosures to authorities.

In relation to establishing a relevant legal basis for data processing, as well as the grounds discussed above (consent, legitimate interests, etc.), the 'legal obligation' basis may be relevant in responding to information requests and investigations by authorities. The GDPR and DPA 2018 provide that personal data may be disclosed to comply with a legal obligation (excluding contractual obligations), but only to the extent necessary to comply with that legal obligation: a proportionality test applies. This ground can only be relied on to justify data processing where a clear and binding legal obligation is present, under national UK or European law. Obligations originating from outside the United Kingdom or Europe do not provide a legal basis for data processing on this ground, even where those obligations may be binding on a non-European entity within an organisation's global corporate group, for example. Organisations should carefully document the relevant legal obligation, and the associated assessment of necessity and proportionality, to evidence GDPR compliance.

In the context of international investigations, companies will need to address the GDPR restrictions and requirements for the transfer of personal data outside the EEA. The considerations for organisations disclosing data to third party authorities are slightly different from those concerning internal investigations. For example, reliance on individual consent or the SCCs is unlikely to be practicable. Transfers necessary to establish or defend a legal claim may be a helpful

48 https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr.

relevant ground in this context, though it is only available for occasional transfers, so may not be appropriate in ongoing investigations or longer-term engagement with authorities. An alternative basis to consider is provided by the GDPR requirements for transferring data under international agreements, such as mutual legal assistance treaties (MLATs).[49] Using MLATs provides a structured system for exchanging information and evidence, but the process can be expensive and lengthy, which is particularly unhelpful where credit for early and responsive co-operation is sought, particularly when dealing with US authorities.

As a general position, companies should be cautious when transferring data, even in response to requests from authorities.

Some national regulators (such as the FCA and the US Securities and Exchange Commission) have reciprocal arrangements in place to transfer data. The use of these inter-regulator arrangements has a number of attractions. However, they often operate through a memorandum of understanding between the regulators, which on its face does not satisfy the definition of a legal agreement under Article 48 of the GDPR and so may not be an appropriate method for data transfer. While the interpretation of Article 48 of the GDPR remains untested, caution should be taken about permitting data to be transferred outside the jurisdiction under a memorandum of understanding between regulators.

See Chapters 11 and 12 on production of information to authorities

An alternative method for complying with the GDPR may be to redact personal information before handing documents over to authorities, depending on the size of the document set. This may, however, be a very expensive way of satisfying the authorities and the GDPR, particularly as it would require not only the data subject's name to be redacted, but also any information from which the data subject could be identified.

Investigations by authorities: US perspective 40.5

As in the United Kingdom, companies in the United States must be mindful of the GDPR's restrictions in responding to subpoenas or other compulsory demands requiring the production of documents. Under US law, a company served with compulsory demands must produce any responsive documents within its possession, custody or control – wherever the data is stored. It is common for US law enforcement agencies or regulators to issue demands for documents to companies requiring the production of large volumes of data. To the extent that responsive data is stored in the European Union, and contains personal data subject to the GDPR, the company must produce it notwithstanding its foreign location. As a result, US companies served with formal demands to produce documents may face a situation where their obligations to comply with US legal process conflict with the GDPR's restrictions.

A US company concerned that it faces such a conflict should first discuss the issue with the regulator or law enforcement agency involved and attempt to narrow the scope of the request to avoid or minimise the need to produce

49 GDPR, Articles 48 and 49.

GDPR-regulated data. This is particularly important because, for the company to rely on the GDPR's legal defence derogation to produce the data to US authorities, the data must be '*necessary* for the establishment, exercise or defence of legal claims'.[50] Accordingly, obtaining clarity from law enforcement or the regulatory agency as to what personal data is necessary to respond to the request, and redacting or otherwise anonymising the other personal data that is not needed, will put a company in a more defensible position if GDPR issues arise.

At the same time, US law enforcement authorities or regulatory agencies are likely to press for clarity as to whether the GDPR genuinely prohibits the transfer of the data in question to US authorities. The US Department of Justice has taken a robust approach previously in similar circumstances, by asserting: 'Where a company claims that disclosure is prohibited, the burden is on the company to establish the prohibition. Moreover, a company should work diligently to identify all available legal bases to provide such documents.'[51] Although the risk of breaching obligations under the GDPR should be a major consideration when dealing with investigating authorities, companies must balance this against the risks of non-compliance with US authorities, which may seek sanctions (including even criminal contempt) against a company for failing to comply with investigators' demands.

Where a company truly cannot comply with a demand for documents from US authorities without violating the GDPR's transfer restrictions, and the company is unable to negotiate an adequate resolution with the US authorities involved, the company may choose to challenge the legal process. US courts have long held that, where it would violate foreign law for a company to produce certain documents in response to US legal process, the company may challenge enforcement based on international comity. If the court agrees that compliance with the demand for documents would give rise to a true conflict of laws, it will weigh the conflicting legal obligations of US law and foreign laws case by case.[52] Specifically, a court entertaining such a challenge must consider, among other things, the importance of the records to the US legal matter for which they are sought, the availability of alternative means of securing the information and the extent to which non-compliance with the request would undermine important interests of the United States, or compliance would undermine important interests of the state where the information is located.[53]

50 Id., at Article 49.

51 https://www.justice.gov/archives/opa/blog-entry/file/838386/download.

52 *Linde v. Arab Bank, PLC*, 706 F.3d 92, 108 (2d Cir. 2013).

53 See *Société Nationale Industrielle Aérospatiale v. United States Dist. Court for S. Dist.*, 482 U.S. 522, 544 n.28 (1987); see also Clarifying Lawful Overseas Use of Data Act (2018), P.L. 115-141 (amending section 2523 of the SCA and codifying the common law comity challenge with respect to compelled process for data served pursuant to the SCA).

However, while courts have sometimes quashed subpoenas on comity grounds in civil litigation,[54] they have typically rebuffed such challenges in the context of criminal investigations, finding that the domestic interest in enforcing the criminal laws trumped the foreign data privacy interests involved.[55] The enforcement of the GDPR and the severe potential penalties that attach to non-compliance may provide greater motivation to companies to challenge US legal process if they believe there is a risk that compliance will run afoul of the GDPR's requirements; and likewise, the prospect of GDPR penalties may lead US courts to give more weight to foreign data privacy interests than they might otherwise in such challenges. Indeed, US court decisions applying the international comity balancing test have sometimes turned, in significant part, on the low likelihood of severe penalties being imposed on the recipient of the legal process at issue if complied with.[56] It is unclear, however, whether and to what extent the GDPR will actually change the equation in this regard – at least prior to a significant fine or other penalty for a disclosure.

Whistleblowers 40.6

The interplay between the increased protections for individuals under the GDPR and the protections for whistleblowers under existing laws is a particularly interesting one for practitioners and companies. More and more, internal and government investigations are triggered by information from (often anonymous) whistleblowers. Senior managers must be acutely aware of the respect to be shown to whistleblowers and whistleblowing laws, in particular with regard to anonymity and protection of the individual.

Whistleblowing policies and data protection 40.6.1

Companies should have in place whistleblowing policies that respect the data protection principles – including specific whistleblower anonymity and privacy protections applicable in some jurisdictions – also providing safeguards for the subject of any whistleblowing report, the whistleblower and any third parties

54 See, e.g., *In re Cathode Ray Tube (CRT) Antitrust Litig.*, 2014 WL 1247770 (N.D. Cal. Mar. 26, 2014); *Motorola Credit Corp. v. Uzan*, 293 F.R.D. 595 (S.D.N.Y. 2013); *Tiffany (NJ) LLC v. Forbse*, 2012 WL 1918866 (S.D.N.Y. May 23, 2012).

55 See, e.g., *United States v. Davis*, 767 F.2d 1025, 1033-34 (2d Cir. 1985) (according deference to judgment of Executive Branch that interest in enforcing criminal laws outweighed interest of Cayman Islands in preserving privacy of its banking customers); *In re Grand Jury Proceedings*, 532 F.2d 404 (5th Cir.), *cert. denied*, 429 U.S. 940 (upholding a grand jury subpoena against comity challenge based on foreign banking privacy laws); *United States v. First City Nat'l City Bank*, 396 F.2d 897 (2d Cir. 1968) (same).

56 Compare, e.g., *First City Nat'l City Bank*, 396 F.2d at 905 (compelling production of records notwithstanding potential conflict with German law, based in part on finding that the 'risk of civil damages [being imposed under German law] was slight and speculative') with, *Tiffany (NJ) LLC v. Qi Andrew, et al.*, 276 F.R.D. 143, 159 (S.D.N.Y. 2011) (declining to compel production given conflict with Chinese banking statute, where history of prosecutions demonstrated that the 'statute has been used to prosecute individuals and that violations can result in serious punishment').

mentioned in the report. Companies will also need to ensure that by default, only personal data necessary for the specific purpose of investigating a whistleblowing report is processed.

40.6.2 Right to access

Where an individual's personal data has been processed during an investigation following a whistleblower report, the individual will still have the rights to access certain information as they would have done in any other circumstances. This includes the purpose and period envisaged for processing and how the data will be stored.[57] The personal information in a whistleblowing report can relate to whistleblowers, the person under investigation, witnesses or other individuals that are mentioned, meaning that companies will need to uphold the data protection rights of all involved.[58]

In addition, under the GDPR, employees may demand any information held about them by their employer. This, the European Data Protection Supervisor has noted, is 'of particular concern in the whistleblowing context as it could, theoretically, risk exposing a whistleblower's identity'.[59] The Article 29 Working Party (now replaced by the European Data Protection Board) has stated that the right to access data may be restricted in order to ensure the whistleblower's rights are protected and '[u]nder no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower from the scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement'.[60] This is reflected in the DPA 2018, which states that companies do not have to comply with a request for access to personal data if it would mean disclosing information about another individual who can be identified from that information, except if the other individual has consented to the disclosure, or it is reasonable to comply with the request without that individual's consent.[61] Therefore, companies may be able to limit access to data following a whistleblower report, but they will still need to balance the data subject's right of access to their personal data against the whistleblower's rights and the rights of any third parties mentioned in the report.[62]

See Chapters 19 to 21 on whistleblowers

57 GDPR, Article 15.

58 European Data Protection Supervisor: 'Whistleblowing' available at https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en.

59 Ibid.

60 Article 29 Data Protection Working Party, Opinion 1/2006, WP117 adopted 1 February 2006, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

61 DPA 2018, Section 45.

62 European Data Protection Supervisor: 'Whistleblowing' available at https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en.

Collecting, storing and accessing data: practical considerations 40.7

A few practical considerations for all investigations:

- Involve data controllers and other relevant organisations at as early a stage as possible.
- Identify any relevant documents to be transferred that contain special category data or any criminal offences data, and document the specific derogations or conditions on which that data will be used.
- Document all decision-making relating to the handling of that data (particularly any assessment of legitimate interests as a lawful basis for processing) and any transfer of that data outside the United Kingdom or the European Union and consider it against Article 49 of the GDPR.
- Work with authorities to agree realistic expectations for the scope and timing of data requests.
- Consider all options for the transfer of data outside the United Kingdom or the European Union, including domestic review, redactions, MLATs and the use of domestic authorities.

41

Directors' Duties: The UK Perspective

Nichola Peters and Michelle de Kluyver[1]

41.1 Introduction

Corporate governance has become increasingly important in the context of financial crime compliance and investigations. One reason for the development is that good corporate governance is a foundation for asserting substantive legal defences to allegations of misconduct. Legislative developments such as the introduction of the UK Bribery Act 2010 and the Criminal Finances Act 2017 mean that the board's responsibilities for identification, mitigation and ongoing review of financial crime risk have a material impact on whether companies can defend allegations of criminal conduct by associated persons (those providing services to the company). The 'adequate procedures' and 'reasonable prevention procedures' defences contained in that legislation require companies to demonstrate 'top-level commitment' to managing financial crime risk and to show that they have understood and managed their financial crime risks proportionately by reference to the nature, scale and complexity of their operations. In the financial services sector, senior managers in firms subject to the Senior Managers and Certification Regime (SMCR) will have specific statements of responsibilities for which they can be held to account.

See Chapter 23 on negotiating global settlements

In 2014 the United Kingdom introduced deferred prosecution agreements (DPAs) as a new mechanism for resolving corporate criminal investigations where there is evidence of criminal conduct. DPAs have added to the focus on corporate governance. Factors that influence whether to offer a company a DPA resolution include whether the company has an effective compliance programme, the composition and conduct of the management team, and the extent to which corporate structures or processes have been changed to mitigate identified risks. A company's prevention procedures are therefore relevant to corporate outcomes even where they fall short of the legislative standard required to establish a substantive

1 Nichola Peters and Michelle de Kluyver are partners at Addleshaw Goddard LLP.

defence. A company's commitment to compliance will also be taken into account in calculating the level of fines or other penalties.

The issue of how companies manage themselves and identify and mitigate their risks has therefore become central in financial crime investigations. Indeed, an investigations process forms part of a company's prevention procedures and companies should take care to ensure that investigations are sufficiently independent and appropriately robust. Where there are allegations of misconduct that may entail significant reputational or commercial risk, the board (or a board subcommittee) is likely to provide oversight of particular investigations, in addition to providing oversight of a company's overall compliance obligations. Directors can also be compelled to give evidence as witnesses in government investigations to explain (among other issues) their company's approach to compliance.[2]

In significant investigations, and subject to managing conflicts of interest, the board is likely to be involved in making strategically important decisions such as whether to self-report suspected misconduct and how to resolve findings of misconduct in a major investigation.

It is therefore important that directors are aware of the multiple sources of their duties and obligations and how they are likely to apply both to the board's oversight obligations regarding the management of financial crime risk and in individual investigation scenarios.

Sources of directors' duties and responsibilities under UK law 41.2

The core duties owed by directors to their companies are set out in sections 171 to 178 of the Companies Act 2006 (CA 2006). Directors may also have additional duties depending on the company they serve. The commentary below identifies and explains the key sources of governance obligations for directors in the United Kingdom. As a result of the global financial crisis and high-profile examples of corporate collapse, the legislative and regulatory framework is increasingly focused on integrity, accountability and driving high standards of business conduct.

Companies Act 2006 41.2.1

The duty to act within powers (section 171 CA 2006) 41.2.1.1

Directors are not permitted to abuse their powers.[3] They must act in accordance with the company's constitution, which includes its articles of associations, resolutions, decisions and investment agreements. In addition, directors are only permitted to exercise their powers for the purposes for which they are conferred, called the 'proper purpose test'. The question of whether a power has been exercised properly will turn on whether the 'substantial' or 'dominant' purpose for

2 Directors can of course also become suspects in an investigation, but this chapter focuses on oversight responsibilities and not directors' individual defence rights.

3 s.171 CA 2006.

which it was exercised was the purpose for which it was conferred.[4] Directors must not exercise their powers to protect their own positions. If power is exercised for a wrongful purpose, the use to which that power is put is voidable.

In the context of a financial crime investigation, it would be an improper use of power if a director sought to prevent, control or influence an investigation to protect his or her own position. A director in this position would also have a conflict of interest, which would engage the separate duty to avoid conflicts of interest. The conduct would also likely breach the duty to promote the success of the company. Investigators must always be alive to the risk of conflicts of interest within the investigation team and in the reporting line.

41.2.1.2 Duty to promote the success of the company (section 172 CA 2006)

The duty to promote the success of the company is relevant to almost everything a director does. The duty requires directors to act in good faith in a way they consider would be most likely to promote the success of the company for the benefit of its members as a whole.[5] The courts will typically respect the decisions of the board provided that they reach the standard of a good-faith business judgment.

When discharging their duties to promote the success of the company, directors must have regard to a list of factors, including:

- the likely consequences of any decision in the long term;
- the interests of the company's employees;
- the need to foster the company's business relationships with suppliers, customers and others;
- the impact of the company's operations on the community and the environment;
- the desirability of the company maintaining a reputation for high standards of business conduct; and
- the need to act fairly as between members of the company.

The list of factors is not exhaustive. Directors may balance the various factors and they must take into account any other factor that would be relevant to a particular decision.[6]

The Association of General Counsel and Company Secretaries of the FTSE 100 (GC100) and the Chartered Governance Institute (ICSA) have published useful, practical guidance notes relevant to the interpretation and application of this duty.[7] The GC100 Guidance on Directors' Duties: Section 172 and Stakeholder Considerations (GC100 Guidance) states that: 'The factors are designed to ensure that, in promoting the success of the company, broader implications of decisions

4 *Howard Smith Ltd v. Ampol Petroleum Ltd* [1974] A.C. 821; *Eclairs Group Ltd v. JKX Oil & Gas Plc* [2015] UKSC 71; [2016] 3 All ER 641.

5 s.172 CA 2006.

6 *Re Phoenix Contracts (Leicester) Ltd* [2010] EWHC 2375 (Ch).

7 The GC100 Guidance on Directors' Duties (2007); The GC100 Guidance on Directors' Duties: Section 172 and Stakeholder Considerations (2018); ICSA Guidance Note Directors' General Duties.

are considered by the directors. You may find it helpful to see the duty as about creating a culture in the business, so that when you take decisions, their wider impact has been considered.'

The duty to promote the success of the company is intertwined with the duty to act with reasonable care, skill and diligence set out in section 174 of the CA 2006. The GC100 Guidance states that: 'The section 172 duty must be fulfilled by a director in accordance with the duty of care, skill and diligence imposed by section 174.'

An interesting application of the duty to promote the success of the company to investigations is that where directors may be implicated in misconduct, they must disclose their own wrongdoing.[8] A director who asserts the privilege against self-incrimination will therefore breach this duty.

In insolvency situations, the interests of creditors will take precedence over the interests of members. This can materially change how the board approaches an investigation. A company's solvency position can change for reasons unrelated to the investigation but also for reasons central to the investigation, such as where there has been an internal fraud. If there are concerns about the company's solvency, directors should proactively seek legal and financial advice as to their altered duties.

Most UK-incorporated companies will have an obligation from their next reporting period (2020) to report on the company's performance of the duty under section 172 of the CA 2006.[9] The government believes that by imposing reporting obligations linked to this duty, directors will consider the wider stakeholder issues more carefully and that boardroom engagement will be improved. In 2018, the Financial Reporting Council (FRC) published its Revised Guidance on the Strategic Report to assist companies in their reporting. It is believed that the enhanced reporting obligations for non-financial information will result in more trust and transparency in business.

See Section 41.2.6

General oversight obligations and oversight of material investigations

The duty to promote the success of the company is central to the directors' obligations to ensure that a company identifies and mitigates its financial crime risks.

The GC100 Guidance recommends that directors ensure that they receive the information they need to carry out their roles and satisfy the duty. In the context of the board's oversight duties in relation to compliance, directors should satisfy themselves that both the quality and frequency of the management information they receive is adequate. Directors need to understand the company's risk profile and risk assessment, and how the compliance programme responds to these risks. In addition, directors should expect to receive periodic reporting to satisfy themselves that the procedures adopted remain fit for purpose. There is no one-size-fits-all approach, and the detail and frequency of management information will depend on the size, complexity and risk profile of the organisation. Data about

8 *Item Software (UK) Ltd v. Fassihi* [2004] EWCA Civ 1244.

9 The Companies (Miscellaneous Reporting) Regulations 2018.

non-material issues and investigations will often be aggregated and shared annually. Where the board has oversight of a material investigation, they are likely to require more detailed information and regular information flows. The company should consider the issue of legal privilege in this regard.

See Chapter 35 on privilege

Where boards are receiving legally privileged advice about investigations or material compliance issues, the way in which it is communicated to the board and documented in the minutes will need to be carefully managed. The GC100 Guidance on Directors' Duties states that directors should not be 'forced to evidence their thought processes' as this would create unnecessary process and 'inevitably expose directors to a greater and unacceptable risk of litigation'.

41.2.1.3 Duty to exercise independent judgment (section 173 CA 2006)

Directors must exercise independent judgment in the interests of their own company,[10] regardless of whether they align with the interests of other group companies. The principle that underpins this duty is that directors must not subordinate their powers to the will of others unless they are authorised to do so under the constitution. Director nominees may therefore follow the instructions of their appointer if the company constitution so allows, provided that they are able to comply with their other legal obligations.

The duty does not prevent directors from seeking and relying on professional advice to form an opinion provided that the decision they reach is their independent judgment.[11] Directors may also delegate their powers (although they remain responsible for their exercise) provided that such a delegation is authorised.

Directors may also be able to fetter their discretion in certain circumstances, provided that it promotes the success of the company to do so. For example, directors could bind the company to an exclusive commercial arrangement and agree to exercise their powers to ensure that the contract was carried out.

41.2.1.4 Duty to exercise reasonable care, skill and diligence (section 174 CA 2006)

Directors must exercise reasonable care, skill and diligence in how they discharge their duties.[12] The standard is both objective (the care, skill and diligence that would reasonably be expected of a director acting with reasonable diligence) and subjective (the general knowledge, skill and experience that the particular director has). As a general rule, a non-executive director will not be expected to have the same level of knowledge of the internal workings of the business that an executive director would.

Directors must satisfy themselves that they have a proper understanding of the functions and duties of directors, the fundamental principles of company law, the company's business, the risks faced by the company and the regulatory and compliance regime in which it operates.[13] Directors should also, as a practical matter,

10 s.173 CA 2006.

11 *Duomatic Ltd, Re* [1969] 2 Ch. 365; [1969] 2 WLR 114; (1968) 112 SJ 922.

12 s.174(2) CA 2006.

13 *Raithatha (as liquidator of Halal Monitoring Committee Ltd) v. Baig* [2017] All ER (D) 244.

ensure that they receive a proper induction and ongoing training to keep their knowledge, skills and experience up to date.

Directors may rely on the expertise of colleagues and advisers in discharging their functions. Indeed, a failure to seek expert advice may amount to a breach of the duty.[14] The right (or duty) to seek advice does not absolve a director from the duty to supervise the discharge of delegated functions.[15] It must be reasonable for directors to rely on the advice of colleagues or advisers.[16] For example, directors must ensure that advisers have appropriate expertise and are instructed to address relevant issues; they should also ensure that advisers are free from conflicts of interest.[17] The question of whether reliance is reasonable will depend on the circumstances.

Although there is no difference between the tests to be applied to executive and non-executive directors, the law recognises that because they fulfil different functions, they will reasonably be expected to exercise different levels of care, skill and diligence. The extent to which a non-executive director may reasonably rely on the executive directors would be fact-sensitive.[18] Non-executive directors should expect to comply with high standards. They would also be expected to properly understand any activity that contributed significantly to a company's commercial offering or revenues.[19]

Duty to avoid conflicts of interest (section 175 CA 2006) 41.2.1.5

Companies are entitled to the benefit of impartial decision-making on the part of their directors. Directors therefore have a duty to avoid actual and potential conflicts between their personal interests and those of the company they serve even where they are acting in good faith.[20] The duty is widely drawn. Section 175 of the CA 2006 states that: 'A director of a company must avoid a situation in which he has, or can have, a direct or indirect interest that conflicts, or possibly may conflict, with the interests of the company.' The reference to indirect interests requires directors to take account of whether persons connected with them[21] might have a conflict of interest.

The application of the duty is acute where it involves the exploitation of a company's property, information or opportunity, and it is immaterial whether the company could itself have taken advantage of the opportunity or whether it suffered any loss. The test is an objective one and directors must therefore

14 *Duomatic Ltd*, above.

15 *Bradcrown Ltd, Re* [2002] B.C.C. 428; [2001] 1 B.C.L.C. 547.

16 *Coleman Taymar Ltd v. Oakes* [2001] 2 B.C.L.C. 749.

17 *Iesini v. Westrip Holdings Ltd* [2009] EWHC 2526 (Ch); [2010] B.C.C. 420; [2011] 1.

18 *Equitable Life Assurance Society v. Hyman* [2002] 1 A.C. 408; [2000] 3 WLR 529; [2001] Lloyd's Rep. IR 99.

19 *Continental Assurance Co of London Plc (In Liquidation), Re*; *Raithatha (as liquidator of Halal Monitoring Committee Ltd) v. Baig* [2017] All ER (D) 244; *Barings Plc (No.5), Re, Secretary of State for Trade and Industry v. Baker* [1999] 1 B.C.L.C. 433.

20 s.175(1) CA 2006.

21 By reference to the list set out in s.252 CA 2006.

analyse whether a reasonable person would think that the relevant facts and circumstances gave rise to a real and sensible possibility of conflict. If the situation cannot reasonably be regarded as giving rise to a conflict of interest, the duty will not be breached.[22]

The duty will not be infringed where the conflict has been authorised in advance by the directors where there is a power to do so in the company's constitution.[23] The authorisation will only be effective if the relevant meeting is quorate without counting any interested directors and the authorisation was given without counting their votes. Effective authorisation will require directors to give full disclosure of the scope and nature of the conflict. In 2008, the GC100 published guidance on Directors' Conflicts of Interest, which includes guidance on authorisation.[24] Directors will not infringe their duties if they act in accordance with provisions in the company's articles for dealing with conflicts of interest.[25]

It may be possible for shareholders to authorise a conflict of interest in advance or subsequently ratify a breach of duty. There are limits on the type of conduct that can be authorised or ratified, and the process that applies will need to be checked taking into account the company's constitution.

41.2.1.6 Duty not to accept benefits from third parties (section 176 CA 2006)

Directors must not exploit their positions for personal benefit (financial or non-financial). The duty provides directors must not accept a benefit from a third party conferred by reason of them being a director or their doing (or not doing) anything as a director.[26] The duty will not be infringed if the acceptance of the benefit cannot reasonably be regarded as likely to give rise to a conflict of interest. The duty is very strict and directors need to take account of these obligations when accepting corporate hospitality or gifts. Although in a bribery investigation the focus will be on whether benefits provided to directors or the company were criminal, it is important not to lose sight of this duty where the conduct concerns individual directors. A company may recover the value of any benefits unlawfully received by a director through civil proceedings, and not just criminal action.

41.2.1.7 Duty to declare an interest in a proposed transaction or arrangement (section 177 CA 2006)

Section 177 CA 2006 requires a director to disclose to the other directors the nature and extent of any interest that the director has in relation to a proposed transaction or arrangement with the company. There is no requirement for authorisation. The term 'arrangement' is wider than the term 'transaction' and includes agreements or understandings having no contractual effect. The interest can be direct or indirect and therefore the interests of connected person must be

22 s.175(4)(a) CA 2006.

23 s.175(4)(b) CA 2006.

24 See also ICSA guidance on Directors' conflicts of interest.

25 s.180(4)(b) CA 2006.

26 s.176 CA 2006.

considered.[27] Directors must disclose the nature and extent of the interest before the company enters into the transaction or arrangement.

Directors do not have to make a declaration where they are unaware of having an interest or are not aware of the transaction or arrangement in question. However, they will be assumed to have knowledge of matters of which they ought reasonably to be aware. Directors will therefore need to undertake a certain amount of due diligence regarding their potential interests to avoid breaching the duty.

If the interest cannot reasonably be regarded as likely to give rise to a conflict of interest, it need not be declared. Further, if the other directors are already aware, or ought reasonably to be aware, of the conflict of interest, it does not have to be declared. Finally, interests relating to a director's service contract need not be declared if they have been considered by a meeting of the directors or a committee appointed for the purpose.

The company's articles may contain provisions for dealing with conflicts of interest compliance that are designed to prevent a breach of the general duty.[28] Section 182 of the CA 2006 deals separately with declarations of interest in existing transactions or arrangements not already declared under section 177.[29]

Other statutory, common law and equitable duties 41.2.1.8

The statutory duties are not exhaustive. Directors of all UK companies also owe a duty of confidentiality to the company and have duties to act fairly as between different members and consider the interests of creditors in appropriate circumstances. Directors also have numerous reporting obligations. Other obligations will depend on the nature of the company.

UK Corporate Governance Code 41.2.2

Companies with premium listings in the United Kingdom are required (for accounting periods beginning on or after 1 January 2019) to state in their annual report and accounts whether they have complied with the UK Corporate Governance Code (2018)[30] and if not, explain the reason. The 'comply or explain' approach is designed to promote transparency about how companies have complied with the high standards of governance set out in the Corporate Governance Code and to promote trust.

The Corporate Governance Code (2018) is the latest iteration of a code that was first published in 1992. The revised code has been developed to respond to a modern business environment in which a key role of the directors is to build relationships with a wider group of stakeholders. The principles set out in the code have been updated to emphasise the link between strong corporate governance and long-term success.

27 See s.252 CA 2006.

28 s.180(4)(b) CA 2006.

29 Breach of s.182 CA 2006 is a criminal offence.

30 https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf.

The Corporate Governance Code is designed around five pillars:

- board leadership and company purpose;
- division of responsibilities;
- composition, succession and evaluation;
- audit, risk and internal control; and
- remuneration.

The Corporate Governance Code sets out a number of principles in relation to each of these items. Although they are all relevant to the identification and management of financial crime risk and the investigation of issues arising, the principles linked to board leadership and company purpose; division of responsibilities; and audit, risk and internal control are the most relevant.

Principles relating to board leadership and company purpose require directors to act with integrity. They must ensure that they establish a framework of prudent and effective controls to assess and manage risk in which the workforce should be able to raise any matters of concern.

The principles linked to the division of responsibilities highlight that the chair should facilitate board relations and the effective contribution of all the non-executive directors. The chair should also ensure that directors receive accurate, timely and clear information. The board must ensure through its composition that no one individual or group dominates the board and that there is a clear division of responsibility between the leadership of the board and the executive leadership of the business.

The principles further provide that non-executive directors must have sufficient time to meet their responsibilities and 'should provide constructive challenge, strategic guidance, offer specialist advice and hold management to account'.[31] The company secretary should support the board to ensure that it has what it needs to function effectively and efficiently. This will include making time and proper information available to the board to discharge its oversight responsibilities.

The principles that underpin the section on audit, risk and internal control are of particular relevance in managing financial crime risk. They state:

> *M. The board should establish formal and transparent policies and procedures to ensure the independence and effectiveness of internal and external audit functions and satisfy itself on the integrity of financial and narrative statements.*
>
> *N. The board should present a fair, balanced and understandable assessment of the company's position and prospects.*
>
> *O. The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.*

31 Principle H, UK Corporate Governance Code.

The audit committee plays a key role in how the company complies with these obligations. The Corporate Governance Code sets out the requirements for the audit committee, which is responsible for, among other items:

> - *reviewing the company's internal financial controls and internal control and risk management systems, unless expressly addressed by a separate board risk committee composed of independent non-executive directors, or by the board itself;*
> - *monitoring and reviewing the effectiveness of the company's internal audit function or, where there is not one, considering annually whether there is a need for one and making a recommendation to the board;*
>
> . . . . .
>
> - *reviewing and monitoring the external auditor's independence and objectivity;*
> - *reviewing the effectiveness of the external audit process, taking into consideration relevant UK professional and regulatory requirements*[32]

The board retains overall responsibility for assessing and managing the company's risks. Boards must carry out a robust assessment of the company's emerging and principal risk, have in place procedures to identify its emerging risks and explain how these are being managed or mitigated. The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.

Separately, the FRC has published Guidance on Audit Committees[33] and Guidance on Risk Management, Internal Control and Related Financial and Business Reporting[34] to assist companies in complying with these principles.

Appendix C of the Guidance on Risk Management, Internal Control and Related Financial and Business sets out the questions the board can ask itself in the context of its risk-related responsibilities, as the small sample of its risk-related questions set out below illustrates:

> *Risk appetite and culture*
>
> - *How has the board agreed the company's risk appetite? With whom has it conferred?*
> - *How has the board assessed the company's culture? In what way does the board satisfy itself that the company has a 'speak-up' culture and that it systematically learns from past mistakes?*

32 Provision 25, UK Corporate Governance Code.

33 https://www.frc.org.uk/getattachment/6b0ace1d-1d70-4678-9c41-0b44a62f0a0d/Guidance-on-Audit-Committees-April-2016.pdf.

34 https://www.frc.org.uk/getattachment/d672c107-b1fb-4051-84b0-f5b83a1b93f6/Guidance-on-Risk-Management-Internal-Control-and-Related-Reporting.pdf.

- *How do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control systems?*
- *How has the board considered whether senior management promotes and communicates the desired culture and demonstrates the necessary commitment to risk management and internal control?*
- *How is inappropriate behaviour dealt with? Does this present consequential risks?*
- *How does the board ensure that it has sufficient time to consider risk, and how is that integrated with discussion on other matters for which the board is responsible?*

. . . . .

Monitoring and Review

- *What are the processes by which senior management monitor the effective application of the systems of risk management and internal control?*
- *In what way do the monitoring and review processes take into account the company's ability to re-evaluate the risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment?*
- *How are processes or controls adjusted to reflect new or changing risks, or operational deficiencies? To what extent does the board engage in horizon scanning for emerging risks?*

Public reporting

- *How has the board satisfied itself that the disclosures on risk management and internal control contribute to the annual report being fair, balanced and understandable, and provide shareholders with the information they need?*
- *How has the board satisfied itself that its reporting on going concern and the longer term viability statement gives a fair, balanced and understandable overview of the company's position and prospects?*

The UK Corporate Governance Code does not override or seek to interpret the general duty under section 172 of the CA 2006 to promote the success of the company. However, it is clear from the above that many of the suggestions for how to identify and manage risk will apply in both the context of the general section 172 duty and also the duty to exercise care, skill and diligence.

41.2.3 QCA Code for smaller listed companies

The QCA Corporate Governance Code[35] is intended to provide small and mid-sized UK quoted companies with a corporate governance framework tailored to their needs and less prescriptive than the UK Corporate Governance Code.

35 https://www.theqca.com/shop/guides/143861/corporate-governance-code-2018-downloadable-pdf.thtml.

It consists of 10 corporate governance principles that companies should follow, along with step-by-step guidance on how to effectively apply them and the related disclosures companies should make. Since September 2018, companies listed on the Alternative Investment Market[36] have been required to adopt and identify a recognised corporate governance code. Companies are also required to set out how they comply with that code or explain their reasons for non-compliance.

The 10 principles are to:

- establish a strategy and business model which promote long-term value for shareholders;
- seek to understand and meet shareholder needs and expectations;
- take into account wider stakeholder and social responsibilities and their implications for long-term success;
- embed effective risk management, considering both opportunities and threats, throughout the organisation;
- maintain the board as a well-functioning, balanced team led by the chair;
- ensure that between them the directors have the necessary up-to-date experience, skills and capabilities;
- evaluate board performance based on clear and relevant objectives, seeking continuous improvement;
- promote a corporate culture that is based on ethical values and behaviours;
- maintain governance structures and processes that are fit for purpose and support good decision-making by the board; and
- communicate how the company is governed and is performing by maintaining a dialogue with shareholders and other relevant stakeholders.

Wates Corporate Governance Principles for Large Private Companies 41.2.4

In recent years, the government has extended its focus on corporate governance to large private companies. This is in recognition that private companies are both a substantial and an expanding part of the economy. Under the leadership of the Wates Committee, the FRC and others have developed the Wates Corporate Governance Principles for Large Private Companies.[37] The guidance sets out six principles that such companies should consider within the context of the company's specific circumstances and then explain how they have addressed them in their governance practices. The guidance exists to assist companies but does not have the same status as the UK Corporate Governance Code, which requires companies to comply or explain why they have not done so.

The two principles most relevant to financial crime investigations are Principles 3 (Director responsibilities) and 4 (Opportunity and risk). Principle 3 requires the board and individual directors to have a clear understanding of their accountability and responsibilities. Principle 3 states that the board's policies and procedures

36 AIM – the international market for smaller, growing companies operated by the London Stock Exchange.

37 https://www.frc.org.uk/getattachment/31dfb844-6d4b-4093-9bfe-19cee2c29cda/Wates-Corporate-Governance-Principles-for-LPC-Dec-2018.pdf.

should support effective decision-making and independent challenge. The responsibility of reviewing the governance processes to confirm that they remain fit for purpose and considering any initiatives that could strengthen the governance of the company reside with the chairman and company secretary. The guidance also emphasises the importance of the integrity of information and that the board papers and supporting information should inform the director what is expected of them on each issue.

Principle 4 states that the board is responsible for a company's overall approach to strategic decision-making and both financial and non-financial risk management, including reputational risk. The board must have oversight of risk and how it is managed, and provide appropriate accountability to stakeholders: 'The size and nature of the business will determine the internal control systems put in place to manage and mitigate both emerging and principal risks. Some companies may decide to delegate to a committee to oversee such matters.'

The guidance further elaborates on the responsibilities of the board as follows:

> *The board should establish an internal control framework with clearly defined roles and responsibilities for those involved. It should agree an approach to reporting, including frequency of reporting and the points at which decisions are made and escalated. Responsibilities may include:*
> - *developing appropriate risk management systems that identify emerging and established risks facing the company and its stakeholders. Such systems should enable the board to make informed and robust decisions, including those associated with material environmental, social and governance matters, such as climate change, workforce relationships, supply chains, and ethical considerations;*
> - *determining the nature and extent of the principal risks faced and those risks which the organisation is willing to take in achieving its strategic objectives (determining its 'risk appetite');*
> - *agreeing how the principal risks should be managed or mitigated and over what timeframe to reduce the likelihood of their incidence or the magnitude of their impact;*
> - *establishing clear internal and external communication channels on the identification of risk factors, both internally and externally; and*
> - *agreeing a monitoring and review process.*

41.2.5 FRC Guidance on Board Effectiveness

In July 2018, the FRC published its revised non-mandatory and non-prescriptive Guidance on Board Effectiveness[38] to assist boards to understand and consider good practice in the context of their corporate governance obligations. The Guidance on Board Effectiveness adopts the same structure as the Corporate Governance

38 https://www.frc.org.uk/getattachment/61232f60-a338-471b-ba5a-bfed25219147/2018-Guidance-on-Board-Effectiveness-FINAL.PDF.

Code. However, there is not space in this chapter to summarise the good practices identified, other than to note that it places a strong emphasis on tone from the top and the continual monitoring of culture. Two important sources of cultural data identified are (1) whistleblowing, grievance and 'speak-up' data and (2) attitudes to regulators, internal audit and employees. The Guidance on Board Effectiveness also suggests taking an integrated approach, noting that resources, internal audit, risk and compliance all have a role to play. Providing examples of questions the board can pose itself on different issues, the Guidance on Board Effectiveness is a rich source of information for those assisting a company with remediation or cultural transformation in the context of an investigation (or outside the investigative process).

Reporting on section 172 compliance and corporate governance generally 41.2.6

The CA 2006 requires that all companies, other than those entitled to the small companies' exemption, prepare a stand-alone strategic report. The statutory purpose of the strategic report is to 'inform the members of the company and help them assess how directors have performed their duty' under section 172 (duty to promote the success of the company for the benefit of members as a whole) and in doing so to have regard to the non-exhaustive range of stakeholder interests and other considerations set out in that section. The strategic report must include an explanation of the principal risks and uncertainties faced by the business and disclose information about a number of issues, including material anti-corruption and anti-bribery issues.

Since 2007, when it first came into force, section 172 has, therefore, enshrined the importance of the consideration of wider interested groups in the creation of a successful business for the benefit of shareholders. However, in light of a number of high-profile examples of poor corporate governance – where there was little evidence that appropriate regard had been had to the needs of a broader range of stakeholders (including employees, suppliers and pension beneficiaries) – the government brought forward The Companies (Miscellaneous Reporting) Regulations 2018 (Reporting Regulations) to fulfil its commitment to strengthen stakeholder voices in boardroom decision-making.

The Reporting Regulations aim to drive greater transparency by requiring companies who must prepare a strategic report (other than those that qualify as medium-sized) to ensure that their strategic reports for each year beginning on or after 1 January 2019 include a statement describing how directors have had regard to the matters set out in section 172(1)(a)–(f) of the CA 2006 when performing their duties under that section. All qualifying companies, including subsidiaries, must report and publish their section 172(1) statements on their websites, whether separately or as part of their annual report. The FRC has revised its Guidance on the Strategic Report accordingly.

The Reporting Regulations also amend the content requirements of the directors' report to require certain companies (meeting different qualifying criteria) to include a basic level of information on their stakeholder engagement. This includes disclosing how the board has had regard to the interests of its UK employees and

to the need to foster the company's business relationships with suppliers, customers and others and, in both cases, explaining the effect, including on the principal decisions taken by the company during the financial year.

While there is a degree of overlap between the section 172(1) statements and the revised content requirements for the directors' report, the government's guidance[39] clarifies that the latter requirements are designed to ensure that company reporting includes information about the 'important aspects of the section 172(1) duty even where directors do not judge the information to be of sufficient strategic importance to be included in the strategic report that year'. Where the board considers its stakeholder engagement information is of strategic importance, it may choose to include that information in its strategic report and not its directors' report, with appropriate cross-referencing in the directors' report.

The Reporting Regulations also impose further enhanced reporting obligations as regards governance arrangements on very large UK-incorporated companies, including subsidiaries, with either more than 2,000 employees globally, or an annual turnover over of £200 million globally and a balance sheet total over £2 billion globally. Premium and standard listed companies which are already required to report on their corporate governance arrangements under the Financial Conduct Authority's (FCA) Disclosure Guidance and Transparency Rules (DTR) 7.2 are not within scope.[40] Premium listed companies are required to apply, and comply or explain their non-compliance with, the provisions of the UK Corporate Governance Code under the FCA's Listing Rules.

Companies in scope must include a statement as part of their directors' report stating which corporate governance code, if any, has been applied and how. If the company has departed from the code, it must set out the respects in which it has done so, and the reasons. If the company has not applied any corporate governance code, the statement must explain why and what arrangements for corporate governance were applied. Statements must also be published on a website maintained by or on behalf of the company.

41.2.7 Senior managers regime

The PRA's and FCA's new regime for supervising and approving the conduct of individuals in regulated firms, the SMCR replaces and extends the previous oversight rules for individuals, the Approved Persons Regime. This is a response to the perceived 'firewall of accountability' protecting senior management from regulatory enforcement. The SMCR is intended to clarify and enhance the division of responsibilities in firms, improve the conduct of all staff and to make disciplinary action against individuals easier for the PRA and FCA (the regulators).[41]

39 Department for Business, Energy and Industrial Strategy, 'Corporate Governance – The Companies Miscellaneous Reporting Regulations 2018 Q&A', November 2018.

40 Community interest companies and charitable companies are also exempted.

41 Firms caught by the SMCR will either report solely to the FCA (solo-regulated) or to both the FCA and PRA (dual regulated). A firm's reporting route will depend on whether it is dual- or solo-regulated.

The SMCR regulates individuals in three segments, divided roughly according to seniority:

- Senior managers are the most senior individuals responsible for managing aspects of a firm's affairs which risk serious consequences for the firm or business in the United Kingdom.[42]
- Certification regulates other individuals in firms who the FCA considers conduct types of roles that carry a risk of significant harm to consumers or the market.[43]
- The conduct rules govern the behaviour of all other employees within firms whose roles relate to regulated or unregulated financial services activity.

There is no territorial limit, so the SMCR can capture individuals based overseas, and is not limited to employees.

Banks, insurers and the largest FCA regulated firms must also submit to the regulators a very detailed 'responsibilities map' of senior individuals, oversight, governance and reporting lines, and a statement of responsibilities for each senior management function manager (SMF manager) setting out what matters that individual is responsible for. The documents must explain to whom certain standard 'prescribed responsibilities' designated by the regulators have been allocated. These documents must be kept up to date.

Only SMF managers are now approved as fit and proper by the regulators: in contrast to the previous approved persons regime, certified persons (who will in many cases include individuals previously approved by the FCA) will now only be certified as fit and proper by their employer firms, not the regulators. Firms must test and confirm the fitness and propriety of SMF managers and certified staff annually. This is likely to lead to more employment claims from staff who lose their certification.

The regulators can take disciplinary action against individuals in any of these three categories for breach of the conduct rules or for being 'knowingly concerned' in the firm's breach of the regulators' rules. In addition to the previous 'knowing concern' test, there is a new statutory test[44] for taking action against a senior manager where: (1) the firm breaches a regulatory rule or requirement; (2) the senior manager was at the time responsible for the activities of the firm where the breach occurred; and (3) the senior manager failed to take reasonable steps to prevent or stop the breach occurring. The test imposes a 'duty of responsibility' on senior managers, which has made the record-keeping of decisions and execution of duties more important.

42 The description set out in s.59ZA of the Financial Services and Markets Act 2000 as amended Financial Services (Banking Reform) Act 2013. This is the legislative provision empowering the PRA and FCA to designate senior manager functions.

43 This paraphrases the description set out in s.63E of the Financial Services and Markets Act 2000 (as amended, ibid.), which is the legislative provision empowering the PRA and FCA to designate certification functions.

44 In s.66A of the Financial Services and Markets Act 2000 (as amended).

Complementary rules on handover arrangements where senior managers depart, notifications of breaches to the regulators, and requirements for detailed regulatory references when certified or senior management staff leave a firm are designed to enhance the effectiveness of the Regime.

The SMCR is already in force for banks and insurers and at the time of writing was due to be extended to all other FCA regulated firms on 9 December 2019, with the senior management requirements coming into force on that date, and firms afforded a further year to December 2020 to certify relevant employees and train staff on the conduct rules.

See Chapter 30 on individual penalties

Consequences of breach

The potential consequences for staff subject to the conduct rules who are found by the relevant regulator to have engaged in misconduct or market abuse include a private warning, public censure, unlimited financial penalty, and in the case of SMF managers a restriction, suspension or prohibition from being an approved person. While some forms of directors' and officers' insurance cover the costs of representing an individual in an investigation, the FCA has drafted rules to ensure a financial penalty is paid by the person on whom it is imposed. GEN 6.1.4A prohibits a regulated firm from paying any financial penalty imposed on an employee, director or partner of the firm or of an affiliated company. GEN 6.1.5 is widely drafted to prohibit insurance arrangements designed to indemnify any person against all or part of a financial penalty.

See Chapter 13 on employee rights

41.3 Conclusion

There are many and varied sources of corporate governance obligations and related duties on boards and companies. Although the standards expected of the board as a collective and directors individually will vary depending on the company (listed, regulated, subject to the SMCR, large, complex and so on) and the issues involved, there is considerable convergence in relation to the types of behaviour that are regarded as constituting good practice for identifying and managing risk (including financial crime risk). Directors must ensure that they understand their duties and obligations and their application to their compliance oversight obligations.

42

Directors' Duties: The US Perspective

Timothy P O'Toole, William P Barry and Margot Laporte[1]

Introduction 42.1

Directors are generally viewed as stewards of the corporation and fiduciaries of the corporation's shareholders. Boards of directors are primarily responsible for overseeing the company, and in exercising these responsibilities, directors must discharge their fiduciary duties of care and loyalty and their obligation to act in good faith. Directors, however, confront increasing litigation risk and regulatory scrutiny in navigating their fiduciary duties and the demands of shareholders in the face of corporate compliance crises and independent investigations. In addition, regulators in the United States and around the world have become increasingly focused on the role of the board and its directors with respect to governance, financial reporting and reinforcing the commitment to a culture of compliance. In this chapter, we discuss the fiduciary duties owed by directors in the context of independent investigations, potential director liability for violations of those duties, and strategic considerations for directors to satisfy their fiduciary duties when faced with compliance crises.

Directors' fiduciary duties 42.2

In the United States, the fiduciary duties and responsibilities of members of boards of directors arise primarily out of state corporate law, both from state statutes and evolving case law (also known as common law).[2] Fundamentally, directors owe

1 Timothy P O'Toole and William P Barry are members, and Margot Laporte is counsel, at Miller & Chevalier Chartered.

2 While civil liability for breaches of fiduciary duties arises under state law, public company directors separately may face federal criminal and civil liability for violations of the federal securities laws. For example, among other violations, public company directors may be held liable for financial

fiduciary duties of care and loyalty to the corporation and are expected to carry out their obligations in good faith.[3] These duties lie at the core of a director's oversight and stewardship responsibilities to the corporation.

42.2.1 Duty of care

The duty of care refers to the obligation of corporate directors to exercise the proper amount of care as they make business decisions on behalf of their corporation. Directors must 'use that amount of care which ordinarily careful and prudent men would use in similar circumstances, [and] consider all material information reasonably available in making business decisions'.[4] To satisfy their duty of care, therefore, directors must, among other things, be knowledgeable about the corporation, its business, its industry and relevant risks, including by regularly reviewing financial statements and inquiring into corporate affairs; remain informed about decisions faced by the board; and engage in meaningful consideration of the issues.[5] If a director 'feels that he has not had sufficient business experience to qualify him to perform the duties of a director, he should either acquire the knowledge by inquiry, or refuse to act'.[6]

Director liability for a breach of the duty of care typically arises in two contexts: (1) 'ill-advised' or grossly negligent board decisions that result in a loss for the corporation; and (2) liability for a loss that arose from an 'unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss'.[7] In the seminal case of *Smith v. Van Gorkom*, the Delaware Supreme Court found that the directors of Trans Union Corporation had breached their duty of care by acting with gross negligence in failing to make an informed decision regarding the sale of the company.[8] The court cited the fact that the board approved the sale without having reviewed a term sheet or any other documentation to support the adequacy of the sale price and that the board relied, without any basis, on the uninformed statements of a director regarding the proposed agreement.[9]

---

reporting and disclosure violations, and insider trading and other fraud violations, under the Securities Act of 1933 (Securities Act) and the Securities Exchange Act of 1934 (Exchange Act). The Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley) and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 also enhanced director liability under federal law for self-dealing and compensation-related violations, among others.

3 *In re Walt Disney Co. Derivative Litig.*, 907 A.2d 693, 745 (Del. Ch. 2005), aff'd, 906 A.2d 2 (Del. 2006) (*Disney*).

4 Id. at 749 (internal quotation marks omitted).

5 See *Francis v. United Jersey Bank*, 432 A.2d 814, 822 (N.J. 1981) (duty to conduct regular review of financial statements); *Barnes v. Andrews*, 298 F. 614, 615 (S.D.N.Y. 1924) (duty to enquire into the corporate business).

6 *Francis*, 432 A.2d at 822 (internal quotation marks omitted).

7 *Disney*, 907 A.2d at 749 (quoting *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959, 967 (Del. Ch. 1996) (*Caremark*) (alterations omitted)).

8 *Smith v. Van Gorkom*, 488 A.2d 858, 881 (Del. 1985).

9 Id. at 874.

Directors are only liable for breach of the duty of care if their conduct has amounted to 'gross negligence', meaning that they demonstrated a 'reckless indifference to or a deliberate disregard of the whole body of stockholders or actions which are without the bounds of reason'.[10] Courts have found that 'directors' actions need not achieve perfection to avoid liability', and that directors do not breach a legal duty simply because they 'failed to act as a model director might have acted'.[11] In most cases, monetary damages are unavailable to plaintiffs alleging breach of duty of care, even if they can demonstrate gross negligence. This is because many states, in response to *Van Gorkom*,[12] enacted statutes permitting corporations to eliminate or limit directors' personal liability for monetary damages for breaches of their duty of care.[13] Significantly, these state laws do not authorise corporations to eliminate or limit directors' personal liability for breaches of their duty of loyalty or good faith obligations, and monetary damages remain available to plaintiffs for such breaches.[14]

See Section 42.3

Duty of loyalty 42.2.2

The duty of loyalty 'mandates that the best interest of the corporation and its shareholders take precedence over any interest possessed by a director, officer or controlling shareholder and not shared by the stockholders generally'.[15] Corporate directors 'are not permitted to use their position of trust and confidence to further their private interests'.[16]

As a 'subsidiary element' of the duty of loyalty, directors must carry out their duties in 'good faith'.[17] The obligation to act in good faith is not an independent fiduciary duty or direct basis for liability, but rather is at the core of the duty of loyalty – 'a director cannot act loyally towards the corporation unless she acts in the good faith belief that her actions are in the corporation's best interest'.[18] A director fails to act in good faith where the director 'intentionally acts with a purpose other than that of advancing the best interests of the corporation, where [the director] acts with the intent to violate applicable positive law, or where [the director] intentionally fails to act in the face of a known duty to act, demonstrating a conscious disregard for [his or her] duties'.[19]

Courts have interpreted the duty of loyalty as giving rise to the duty to exercise oversight in the day-to-day business operations of the corporation. The Delaware Court of Chancery set forth the standard for directors' obligation to oversee and

10 *Disney*, 907 A.2d at 750 (internal quotations marks omitted).

11 *Cooke v. Oolie*, Civ. Action No. 11134, 2000 Del. Ch. LEXIS 89, at *58–59 (Del. Ch. 24 May 2000).

12 *Disney*, 907 A.2d at 751.

13 See, e.g., Del. Code Ann. tit. 8, § 102(b)(7).

14 See, e.g., id.

15 *Disney*, 907 A.2d at 751 (internal quotation marks and alteration omitted).

16 *Guth v. Loft, Inc.*, 5 A.2d 503, 510 (1939).

17 *Stone v. Ritter*, 911 A.2d 362, 369 (Del. 2006).

18 Id. at 370.

19 Id. at 369.

monitor the corporation in *In re Caremark International Inc Derivative Litigation*, holding that directors have an affirmative duty to establish a reporting system and internal controls, and to monitor and oversee internal compliance activity.[20] Directors must assure themselves that the system of internal controls is 'reasonably designed' to allow senior management and the board to reach 'informed judgments concerning both the corporation's compliance with law and its business performance'.[21] Failure to do so, the court held, may 'render a director liable for losses caused by non-compliance with applicable legal standards'.[22]

Thus, while 'directors' good faith exercise of oversight responsibility may not invariably prevent employees from violating criminal laws, or from causing the corporation to incur significant financial liability or both',[23] directors are expected to take steps to implement reasonable reporting, information and compliance systems, and to address corporate misconduct of which they become aware.[24]

42.2.3 Oversight obligations under US securities laws

In addition to the standards articulated in *Caremark* and its progeny, the Sarbanes-Oxley Act of 2002 sets expectations for public company audit committees (and consequently the independent directors that serve on audit committees) with respect to their oversight of companies' accounting, internal controls and auditing matters. These include oversight of the company's independent auditors, review of audit reports and the establishment of procedures to address complaints regarding the company's accounting and financial reporting.[25] Audit committees may also hire independent counsel to assist them in fulfilling their responsibilities, including in independent audit committee investigations and compliance reviews.[26]

42.3 Liability for breach of fiduciary duties

42.3.1 Caremark claims in private civil actions

Directors may be subject to civil action in their personal capacity by shareholders of the corporation, both directly and in derivative suits on behalf of the corporation, for alleged breaches of their fiduciary duties. Courts make liability determinations on a director-by-director basis, rather than on the basis of the conduct

20 *Caremark*, 698 A.2d at 970.

21 Id.

22 Id.

23 *Stone*, 911 A.2d at 373.

24 Id. at 370.

25 Sarbanes-Oxley, Pub. L. No. 107-204, 116 Stat. 745, § 301.

26 Id.

See Chapter 34 on parallel civil litigation

of the board as a whole.[27] In most US states, the remedy for breach of a fiduciary duty can be '[a]ny form of equitable and monetary relief'[28] that the court finds 'appropriate'.[29]

Caremark established the standard of liability for alleged breaches of directors' duty of oversight, holding that 'only a sustained or systemic failure of the board to exercise oversight – such as an utter failure to attempt to assure a reasonable information and reporting system exists – will establish the lack of good faith that is a necessary condition to liability'.[30] *Caremark*, therefore, 'articulates a standard for liability for failures of oversight that requires a showing that the directors breached their duty of loyalty by failing to attend to their duties in good faith'.[31] Liability is premised on plaintiffs' demonstration that 'the directors were conscious of the fact that they were not doing their jobs'.[32]

In *Stone v. Ritter*, the Delaware Supreme Court affirmed the standard for oversight liability articulated in *Caremark*[33] and held that a *Caremark* claim for director oversight liability requires the following conditions predicate: (1) that the directors 'utterly failed to implement any reporting or information system or controls'; or (2) that the directors, 'having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention'.[34] In either instance, directors can only be liable if plaintiffs demonstrate that they knowingly violated their fiduciary obligations.[35]

While *Caremark* and *Stone* set a high standard for establishing liability for breach of oversight obligations, board processes and decision-making nonetheless can result in director liability. In *Wells Fargo & Co Shareholder Derivative Litigation*, for example, the plaintiffs alleged that the defendant directors 'knew or consciously disregarded' that Wells Fargo employees were fraudulently creating millions of deposit and credit card accounts for customers as part of 'cross-selling' activities.[36] In denying Wells Fargo's motion to dismiss, the court relied on allegations that the board had been informed of multiple 'red flags' of improper conduct, including alleged communications between employees and board members regarding the fraudulent activity, several related lawsuits, news reports,

27 *Disney*, 907 A.2d at 748.

28 *In re Tri-Star Pictures, Inc. Litig.*, 634 A.2d 319, 333 (Del. 1993) (internal quotation marks omitted).

29 *Cinerama, Inc. v. Technicolor, Inc.*, 663 A.2d 1156, 1166 (Del. 1995) (internal quotation marks omitted). Often, directors' liability for monetary payments will be covered by directors and officers liability insurance.

30 *Stone*, 911 A.2d at 369 (internal quotation marks omitted).

31 *Guttman v. Huang*, 823 A.2d 492, 506 (Del. Ch. 2003).

32 Id.

33 *Stone*, 911 A.2d at 369.

34 Id. at 370.

35 Id.

36 *In re Wells Fargo & Co. S'holder Derivative Litig.*, 282 F. Supp. 3d 1074, 1082 (N.D. Cal. 2017) (*Wells Fargo*).

investigations by government agencies, employee terminations allegedly aimed at silencing whistleblowers, and emphasis on the importance of cross-selling practices in the bank's financial reports.[37] The court found that the numerous red flags alleged 'collectively supported an inference that a majority of the Director Defendants consciously disregarded their fiduciary duties despite knowledge regarding widespread illegal account-creation activities, and that there is a substantial likelihood of director oversight liability'.[38]

42.3.2 The business judgment rule

The 'business judgment rule' is a standard of judicial review that protects directors from personal civil liability for their decisions as long as the decision was independent, informed, made in good faith, with due care and with the honest belief that the action taken was in the company's best interest.[39] The business judgment rule presumes that 'in making a business decision the directors of a corporation acted on an informed basis, . . . and in the honest belief that the action taken was in the best interests of the company [and its shareholders]'.[40] Therefore, the business judgment rule presupposes that directors have complied with their duty of loyalty to the corporation. In the absence of evidence to the contrary, the board's 'decision will be upheld unless it cannot be attributed to any rational business purpose'.[41] If plaintiffs fail to rebut the presumption, they will not be entitled to any remedy, unless the transaction constitutes corporate waste.[42]

Plaintiffs may rebut the presumption by showing that the directors breached one of their fiduciary duties of loyalty or care in connection with the transaction at issue.[43] In that case, the burden shifts to the director defendants to demonstrate that the challenged transaction was 'entirely fair to the corporation and its shareholders'.[44]

Even if directors have exercised their business judgment, the protections of the business judgment rule will not apply if the directors have made an 'unintelligent or unadvised judgment'.[45] Furthermore, the protections of the business judgment rule will not apply in the event of director inaction, unless the directors made a conscious decision not to act.[46] For this reason, it is critical that boards and directors work with management to develop a process that (1) enables the board to obtain the information it needs in order to evaluate and decide on a course of

37 Id. at 1088.

38 Id. (alterations omitted); see also id. at 1107 to 1109.

39 See *Gantler v. Stephens*, 965 A.2d 695, 705–06 (Del. 2006).

40 *Aronson v. Lewis*, 473 A.2d 805, 812 (Del. 1984).

41 *Disney*, 907 A.2d at 747 (internal quotation marks omitted).

42 Id.

43 Id.

44 Id.

45 Id. at 748 (internal quotation marks omitted).

46 Id.

action, (2) facilitates careful consideration and debate at the board level consistent with fiduciary obligations and (3) results in a record that demonstrates the board's execution of its responsibilities.

Regulatory enforcement actions 42.3.3

In addition to being named in securities class action or derivative suits, public company directors can be subjected to regulatory investigations and enforcement actions under US securities laws. Indeed, directors increasingly face all three proceedings – securities class actions, derivative litigation and enforcement proceedings – in parallel. The Securities Exchange Act of 1934 (the Exchange Act), as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act, authorises the US Securities and Exchange Commission (SEC) to institute administrative and civil proceedings and to seek monetary and injunctive relief from directors for their violations of the securities laws.[47] The SEC also can request that a court permanently or temporarily bar an individual from serving as a public company officer or director for violations of the anti-fraud provisions of the US securities laws.[48] In addition, the US Department of Justice (DOJ) can criminally prosecute directors for 'willful' or 'knowing' violations[49] of the US securities laws or conspiracy to commit such violations.[50]

There are clear and direct consequences for companies when oversight is found lacking. In evaluating corporate compliance programmes, regulators focus on the types of information that the board has examined in its exercise of oversight in the area in which misconduct occurred. US regulators have been vocal in commenting on the roles and responsibilities of directors, and have been critical of boards of directors that, in their view, failed to exercise reasonable oversight.[51] The SEC and DOJ have been particularly outspoken with respect to financial reporting and Foreign Corrupt Practices Act (FCPA) matters. In the settlement made with Sociedad Química y Minera de Chile (SQM) for internal controls and books-and-records violations under the FCPA in 2017, for instance, the DOJ explicitly noted

47 Exchange Act §§ 21(a)(1), (d)(3), (d)(5), 15 U.S.C. §§ 78u(a)(1), (d)(3), (d)(5).

48 Id. § 21(d)(2), 15 U.S.C. § 78u(d)(2).

49 Securities Act § 24, 15 U.S.C. § 77x; Exchange Act §§ 13(a), 32(a), 15 U.S.C. §§ 78m(b)(4) and (5), 78ff(a). The securities laws define 'knowing' violations as being 'aware' that one is engaging in conduct, that circumstances exist, or that a result is substantially certain to occur, or having a firm belief of the same. 15 U.S.C. § 78dd-1(f).

50 Sarbanes-Oxley § 902(a), 18 U.S.C. § 1349.

51 See, e.g., Mary Jo White, Chair, US Securities and Exchange Commission, Address at the Stanford University Rock Center for Corporate Governance: A Few Things Directors Should Know About the SEC (23 June 2014) ('One question we are often asked is whether some of the things we are doing may actually discourage strong directors from serving on boards because of the risk that they may unfairly find themselves on the wrong end of an SEC enforcement action. While we do bring cases against directors, these cases should not strike fear in the heart of a conscientious, diligent director').

that although SQM's board had been briefed on certain internal controls failures flagged by internal audit, 'no adequate changes were made to SQM's internal accounting controls'.[52]

Of particular relevance to public company directors, Section 20(a) of the Exchange Act provides that every person who indirectly or directly controls another person found liable for a securities violation under the Exchange Act is liable for that same conduct.[53] For 'control person' liability to attach, the majority of US circuit courts require only that the director exercised control over the general operations of the business that included the violation and could exercise control over the transaction or activity giving rise to it.[54] Section 20(a) provides an affirmative defence to a director who 'acted in good faith' and 'did not directly or indirectly induce' the act constituting the violation.[55]

For example, in 2009, the SEC filed a settled enforcement action against Nature's Sunshine Products, its chief executive officer (CEO) and board member, and its chief financial officer (CFO), alleging that the CEO/director and CFO, in their capacities as control persons under Section 20(a), violated the books-and-records and internal controls provisions of the FCPA.[56] Notably, the SEC did not allege that these individuals had direct knowledge of, or participated in, the underlying improper payments or accounting failures, but rather that the executives failed to identify certain red flags that would have alerted them to the improper payments and failed to perform their corporate duties adequately and in good faith.[57]

42.4 Duty of oversight in investigations

Directors' duty of oversight, and their obligation to act in good faith, are implicated at multiple stages of a corporate investigation – from the decision whether to initiate an investigation, to the decision whether to self-disclose potential wrongdoing to regulators, to decisions authorising negotiation or settlement with regulators. At each stage, directors will need to ask appropriate questions, obtain sufficient information and engage in meaningful consideration to satisfy themselves that the decision is in the best interests of the corporation. Increasingly, independent auditors threaten to initiate reporting procedures under Section 10A of the Exchange Act absent an independent investigation into suspected wrongdoing.[58]

52 *United States v. Sociedad Química y Minera de Chile, S.A.*, No. 1:17-cr-00013, Deferred Prosecution Agreement (D.D.C. 13 January 2017).

53 Exchange Act § 20(a), 15 U.S.C. § 17t(a).

54 See, e.g., *In re Mut. Funds Inv. Litig.*, 566 F.3d 111, 129–30 (4th Cir. 2009); *Laperriere v. Vesta Ins. Group*, 526 F.3d 715, 723–25 (11th Cir. 2008).

55 Exchange Act § 20(a), 15 U.S.C. § 17t(a).

56 *U.S. Sec. Exch. Comm'n v. Nature's Sunshine Prods., Inc.*, Civ. No. 2:09CV0672, Compl. (D. Utah 31 July 2009).

57 Id.

58 Exchange Act § 10(A), 15 U.S.C. § 78j-1.

In addition, directors must consider that, in the event the corporation is prosecuted for misconduct, the board's execution of its duty of oversight will be considered by prosecutors and the court in sentencing the corporation.[59]

Moreover, directors play a central role in the remediation process that often results from an investigation. Directors must oversee the process of enhancing or establishing internal controls for financial reporting or other material aspects of the company's compliance infrastructure that are found lacking. This often requires directors to adapt to, and sometimes reassess, their view of company processes and the conduct of management based on facts developed during an investigation. At the same time, directors must interact with external auditors in connection with the issuance of an audit opinion and oversee a financial reporting process that contemplates such changes.

Often, director liability for breach of fiduciary duty arises from the alleged failure of the board to respond to red flags of corporate misconduct. When faced with actual knowledge or red flags of wrongdoing, directors must take good-faith steps to conduct reasonable inquiry to understand the cause and scope of the issue, and to implement appropriate remediation, as necessary. Directors may be subject to oversight liability on the basis of inaction, wilful ignorance or failure to investigate and address possible misconduct in good faith.

As reflected in *Wells Fargo*, there are numerous ways in which a director may be considered to be on notice of possible wrongdoing at the corporation.[60] These include internal and external audit reports, whistleblower complaints, consumer complaints, news reports, regulatory investigations and related civil litigation claims. The case law emphasises the need for directors to respond to repeated signs of misconduct, as courts and regulators may interpret the absence of a response as a conscious disregard of the directors' duty of oversight. As the Delaware Court of Chancery explained, 'a *Caremark* plaintiff can plead that "the directors were conscious of the fact that they were not doing their jobs," and that they ignored "red flags" indicating misconduct in defiance of their duties. A claim that an audit committee or board had notice of serious misconduct and simply failed to investigate . . . would survive a motion to dismiss, even if the committee or board was well constituted and was otherwise functioning'.[61]

Importantly, by virtue of the audit committee's oversight of accounting, internal controls and auditing matters, the independent directors naturally receive information regarding the corporation's internal controls and compliance system that implicates their duty of oversight. This level of knowledge could subject the

59 See U.S. Fed. Sentencing Guidelines Manual § 8B2.1(b)(2)(A) ('The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance program.').

60 *Wells Fargo*, 282 F. Supp. 3d at 1088, 1107–09.

61 *Shaev Profit Sharing Account v. Armstrong*, C.A. No. 1449-N, 2006 Del. Ch. LEXIS 33, at *16 (Del. Ch. 13 February 2006).

independent directors to increased risk of regulatory scrutiny and private shareholder action if they fail to respond to internal control deficiencies and red flags of potential misconduct that are reported to them.

42.5 Strategic considerations for directors

While there is no effective one-size-fits-all approach to satisfaction of fiduciary duties, directors can take certain steps to meet the ongoing challenges and expectations of regulators and shareholders. Implementation of these strategies may not eliminate the risk of director liability, but they will demonstrate directors' adherence to the core principles of their fiduciary duties.

- *Risk-based compliance framework*: Directors should require management to demonstrate that the company has adopted an effective risk-based compliance framework to identify high-risk compliance issues and prioritise resources accordingly.
- *Remaining informed*: Directors should implement a formal process that facilitates communications between the board and management regarding the compliance framework and business performance. Directors should remain informed about ongoing and acute risks, as well as about the broader business environment and industries in which the company is operating.
- *Independent investigations and compliance crises*: Directors should establish a crisis management strategy and investigative protocol before such measures are needed, including a framework for the board's response if an independent investigation is necessary. This may include proactive delegation of oversight responsibility to the company's audit committee or a special litigation or investigation committee. This also may include an annual presentation from management, including the legal and compliance functions, as to the company's readiness if a government inquiry, whistleblower complaint or other occurrence gives rise to consideration of an independent investigation.
- *Training*: Directors should have sufficient training not only to be familiar with principles of corporate governance and the corporation's business, but also to provide directors a basis from which they can ask questions regarding compliance risks and analyse responses consistent with their oversight responsibilities.
- *Overseeing the external auditor relationship*: The audit committee owns the relationship with the external auditor. Too often, directors limit their interaction with the external auditor to engagement of the auditor and a quarterly discussion in advance of the issuance of a filing. The better course is for independent directors, particularly those on the audit committee, to establish a deeper relationship that provides for a foundation of trust and familiarity from which both parties can act when an unexpected problem arises.
- *Making the record*: A documented approach to corporate governance and adherence to fiduciary duties can mitigate directors' risks in the event of litigation or an enforcement proceeding. Real-time documentation, including through minutes of audit committee or special investigative committee

meetings, are critical evidence of directors' fulfilment of their oversight obligations in the context of a board committee's evaluation of issues involving investigations and compliance crises.

Effective board processes enable directors to execute their responsibilities in accordance with applicable fiduciary duties and the expectations of regulators and the market. Adherence to sound principles of corporate governance protects directors and promotes tangible benefits to the company in the form of:

- heightened investor confidence and corporate reputation;
- increased efficiency and avoidance of costly investigation due to early issue spotting and risk mitigation; and
- higher levels of customer and employee retention.

Appendix 1

About the Authors

Jennifer L Achilles
Reed Smith LLP

Jennifer Achilles is a partner in Reed Smith's global regulatory enforcement group based in New York. Her practice focuses on white-collar criminal defence, securities litigation and internal investigations. Jennifer is regularly ranked as a super lawyer and is an active supporter of diversity initiatives. She defends public and private companies, as well as their officers and directors, in insider trading, market manipulation, fraud, antitrust and Foreign Corrupt Practices Act investigations by the SEC, CFTC, FINRA, DOJ and New York DA's and AG's offices. Jennifer also leads internal investigations in advance of and in connection with government investigations, and counsels clients on co-operation and self-disclosure strategies.

Ama A Adams
Ropes & Gray LLP

Ama A Adams is a litigation and government enforcement partner at Ropes & Gray in Washington, DC. Her practice focuses on international transactions and the US government's regulation of trade and investment. This includes, most notably, export controls, economic sanctions, anti-corruption, foreign direct investment and customs laws and regulations. In addition to advising clients on the application of international trade regulations to their business operations, Ms Adams also assists clients in developing compliance programmes, handling pre- and post-acquisition due diligence, conducting internal investigations relating to potential violations of trade laws and representing clients before the US government agencies in connection with enforcement matters and government inquiries. She advises companies in a range of industries, including the oil and gas, aviation, pharmaceutical, manufacturing, technology, chemical and financial sectors.

Pamela Alarcón
Philippi Prietocarrizosa Ferrero DU & Uría – PPU

Pamela Alarcón is a partner at PPU and an expert in criminal law and compliance. She is also an attorney and consultant in criminal law, corporate criminal law, corruption, crime prevention and compliance, as well as risk analysis in corporate business and criminal litigation. She has an outstanding reputation for managing crises arising from criminal activities within companies, by advising legal representatives, chief executive officers, managers and administrators. She is also a criminal consultant and provides risk analysis in real estate, financial, M&A and infrastructure related matters, among others. She has extensive experience in economic criminal law, as well as corruption and criminal compliance issues.

Pamela has law and political science degrees from Los Andes University, a master's degree in advanced studies of human rights from the Carlos III University in Madrid and a specialist degree in corporate law from Pontifical Xavierian University in Bogotá. She is a former adviser to the Office of the Deputy Attorney General and a professor of corporate criminal law and compliance at various universities in Bogotá.

Stuart Alford QC
Latham & Watkins

Stuart Alford QC is a partner in the London office of Latham & Watkins and a member and former co-chair of the firm's litigation and trial department in London. Mr Alford focuses on economic crime and regulatory matters, leveraging his former experience as one of the UK's leading prosecutors to represent clients in their most critical, high-stakes cases.

From 2012 to 2016, Mr Alford headed the Fraud Division at the Serious Fraud Office (SFO), where he was responsible for many of the UK's landmark white-collar cases. His work focused on investigations in banking and money markets, including the wide-ranging cases involving foreign-exchange benchmarks, a major criminal recapitalisation investigation and the Bank of England's liquidity auctions.

Mr Alford has handled numerous multi-jurisdictional investigations, with a concentration on cross-border US–UK matters. He has supervised case teams prosecuting the LIBOR investigations and trials; led the pre-investigation stages of the foreign exchange manipulation cases and supervised the investigation of liquidity auctions run by the Bank of England during the financial crisis of 2007 and 2008.

He was appointed Queen's Counsel in 2014, while working at the SFO, a rare achievement for a lawyer in public service.

Ami Amin
BCL Solicitors LLP

Ami Amin is an associate whose practice covers both business crime and extradition. She has experience in SFO cases involving allegations of bribery and corruption, and in acting for individuals facing proceedings with an international dimension, particularly in matters relating to the Proceeds of Crime Act 2002.

Before joining BCL, Ami was an associate at a leading London criminal defence firm in its regulatory department. She is an experienced litigator with a background in representing professionals facing disciplinary proceedings.

Anupreet Amole
Brown Rudnick LLP

Anupreet Amole is a partner in Brown Rudnick's white-collar crime and regulatory investigations group. Anupreet has handled sensitive investigations in a wide range of multi-jurisdictional business crime matters, many involving allegations of bribery and corruption, fraud, misuse of confidential information, tax evasion and money laundering. Anupreet has particular experience in advising companies on financial crime compliance policies and procedures, including in the context of M&A deals. Past and present clients include various FTSE 100 companies, senior executives, investment advisory firms, professional services firms and high net worth individuals. In addition, Anupreet is co-leader of the firm's cybersecurity group, advising on legal issues both before and after a data incident. Before joining Brown Rudnick in January 2017, Anupreet was a senior associate at Freshfields Bruckhaus Deringer in London. Anupreet is listed in the 2019 and 2020 editions of *The Legal 500 UK*.

Ilias Anagnostopoulos
Anagnostopoulos

Ilias G Anagnostopoulos has appeared as lead counsel in most of the significant corporate and criminal cases in Greece during the past 30 years and is a professor of criminal law and criminal procedure at the School of Law, National University of Athens. He has extensive experience in most types of business crime, financial fraud, European criminal law, tax and customs fraud, healthcare and procurement fraud, medical malpractice, product criminal liability, environmental liability, compliance, money laundering, corruption practices, anti-competitive practices and cartel offences, anti-terrorism, extradition and mutual assistance. His many publications in Greek, English and German deal with matters of Greek, European and international criminal law, business and financial crimes, reform of criminal procedure and human rights.

He is chair of the Hellenic Criminal Bar Association (since 2013) and a member of the Criminal Law Committee of the Council of the Bars and Law Societies of Europe (chair, 2007–2013), the Criminal Law Experts Commission (Ministry of Justice), the High Legal Council with the Bank of Greece, and FraudNet Commercial Crime Services of the International Chamber of Commerce.

Jodi Avergun
Cadwalader, Wickersham & Taft LLP

Jodi Avergun is the chair of Cadwalader, Wickersham & Taft LLP's white-collar defence and investigations group, based in the firm's Washington, DC, office. Her practice focuses on representing corporations and individuals in criminal and regulatory matters involving, among other things, the Foreign Corrupt Practices Act (FCPA). Her experience in FCPA matters includes directing due diligence reviews in connection with mergers and acquisitions in a number of industries and jurisdictions; designing and implementing robust FCPA compliance policies, systems and training for corporate clients; and counselling clients in voluntary disclosures of FCPA violations. Jodi also advises clients in securities enforcement, healthcare and other white-collar matters, and has successfully represented both companies

and senior executives in internal investigations, matters before regulatory bodies, including the SEC, and civil and criminal matters in federal court.

Jodi was an Assistant US Attorney and senior trial counsel in the US Department of Justice for 17 years. She was recognised in the 2014 edition of *The Legal 500 US* as a 'Key Individual' in the white-collar criminal defence area, and was named one of the 2016 '150 Women in White Collar' by *Corporate Crime Reporter*. Additionally, Cadwalader was named a 'Highly Recommended' firm for FCPA by *Global Investigations Review* in its 2016 rankings of the FCPA Bar in Washington, DC.

Amanda L Azarian
Jenner & Block LLP

Amanda Azarian is an associate at Jenner & Block's London office focusing on investigations, compliance and defence. Ms Azarian has extensive experience in working on a range of government enforcement actions in the United States and United Kingdom, including large, complex matters involving the SFO, NCA, DOJ, SEC and OFAC, with a concentration on economic crime. Her practice includes the representation of both corporates and individuals, conducting and advising on global internal investigations, defending against allegations relating to financial crime and responding to government requests, offering compliance advice including in relation to anti-bribery and corruption, anti-money laundering, and sanctions and developing and implementing tailored compliance programmes, due diligence and risk assessments. Prior to joining Jenner & Block, Ms Azarian worked for the Washington, DC, and London offices of an international law firm. Ms Azarian received her law degree from the Catholic University of America, Columbus School of Law, where she served as a staff member of the *Catholic University Law Review* and interned for the Hon. Heidi Pasichow at the Superior Court for the District of Columbia. She is admitted to practise in both Maryland and Washington, DC.

Kevin Bailey
Brunswick Group LLP

Kevin Bailey is a partner in Brunswick's Washington, DC, office focusing on litigation and crisis communications and related reputational issues. Kevin has spent nearly two decades counselling major corporate clients at reputational crossroads, often against the backdrop of Congressional, SEC or other federal government investigations. Prior to joining Brunswick, Kevin served as BP's head Washington lawyer for over seven years and was a key strategist on the company's response to myriad issues related to the Deepwater Horizon accident in the Gulf of Mexico. Kevin also helped to shape BP's public affairs strategies across the United States and served as a key risk management adviser to executives and members of the board of directors for nearly a decade. Before he joined BP, Kevin practised law at WilmerHale in Washington and represented dozens of major companies before Congress and government agencies and in complex litigation.

Alex Bailin QC
Matrix Chambers

Alex Bailin QC is a barrister with extensive experience in business crime, extradition and media law. He is highly recommended by the legal directories in eight practice areas including business and financial crime, extradition and media law. He was previously a derivatives trader in the City. He has represented and advised a number of corporates and high-profile individuals in business crime cases, including many cross-border cases and those involving parallel civil claims.

Michael Barba
BDO USA, LLP

Michael Barba leads BDO USA LLP's national security compliance practice. Michael has led numerous engagements in transactions involving foreign direct investment and critical infrastructure. He has been appointed as an independent and neutral third-party monitor and security officer reporting directly to the Committee on Foreign Investment in the United States (CFIUS) Monitoring Agencies. He also serves as the independent and neutral third-party auditor of a Tier 1 telecommunications company to assess compliance with CFIUS national security agreement mitigation requirements.

Michael's responsibilities include assessing and analysing national security agreements, interim orders and letters of assurance while developing customised work plans that are approved by the US government.

Michael's responsibilities also extend into BDO's forensic technology services group, where he has more than 20 years' experience in managing complex investigations involving high-tech crime, misconduct and network security incident response. Michael has led BDO's digital forensics and incident response practices in conducting domestic and international investigations affecting the computer networks, resources and intellectual property of numerous Fortune 500 organisations. He received the prestigious High Technology Crime Investigation Association Award for 'The Most Significant High Technology Case' involving public and private sector cooperation.

William P Barry
Miller & Chevalier Chartered

William Barry regularly advises boards of directors, companies and financial institutions on a broad range of issues involving white-collar and securities enforcement, transactional due diligence and compliance with Foreign Corrupt Practices Act, money laundering, economic sanctions and insider trading requirements. Mr Barry guides clients through the complex issues involved in responding to inquiries from domestic and international regulators regarding issues of accounting fraud, foreign bribery, money laundering and other financial crimes. He represents clients faced with the challenge of responding to competing demands in parallel proceedings, such as internal reviews, government investigations and private civil actions.

Milos Barutciski
Borden Ladner Gervais LLP

Milos Barutciski has represented Fortune 500 clients and companies listed on the Toronto Stock Exchange, the New York Stock Exchange, NASDAQ, and European and Asian stock exchanges in anti-corruption, sanctions, export control, cartel, government procurement, money laundering and other regulatory investigations and compliance matters. He has represented clients in investigations by the Royal Canadian Mounted Police, the Canada Border Security Agency, the Competition Bureau, the Ontario Securities Commission and other agencies, including investigations by the US Department of Justice, the US Securities and Exchange Commission and the European Commission. Milos has represented clients in several World Bank corruption investigations and has appeared as counsel before the Bank's Sanctions Committee.

Milos is a founding member of the Task Force on Bribery and Corruption of the Business and Industry Advisory Committee to the OECD in respect of the 1997 Anti-Bribery Convention. He also advised the government of Canada with respect to the drafting of the Corruption of Foreign Public Officials Act. From 1996 to 1999, Milos was engaged by the World Bank to advise on regulatory reform in the Middle East and Africa. He is a member of the executive board of the International Chamber of Commerce. He is called to the bars of Ontario and Quebec.

Claudio Bazzani
Homburger

Claudio Bazzani is a partner and co-head of Homburger's white collar and investigations team and litigation and arbitration practice. He specialises in internal and regulatory investigations and advises corporate clients in compliance matters. He represents clients in investigations by Swiss and foreign authorities as well as in domestic and international litigation and arbitration proceedings.

Claudio Bazzani has more than 10 years of experience in conducting large-scale internal and regulatory investigations. He regularly advises and represents clients in financial market compliance issues and has profound knowledge of the legal and practical challenges Swiss companies face in cross-border matters.

Sara Berinhout
Ropes & Gray LLP

Sara Berinhout is an associate in Ropes & Gray's Boston office and is a member of the firm's litigation department.

Benjamin A Berringer
Clifford Chance US LLP

Benjamin Berringer is an associate at Clifford Chance US LLP, where he focuses on cross-border investigations and complex commercial litigation. Ben represents both corporations and individuals in connection with regulatory investigations before the Commodity Futures Trading Commission, the Department of Justice, and the Securities and Exchange

Commission. Ben also advises on matters arising under cybersecurity, privacy and data protection laws. Ben received his BA from Williams College, his MS in economics from SOAS, and his JD from NYU School of Law.

Eike Bicker
Gleiss Lutz

Dr Eike Bicker is a partner and co-head of the compliance and investigation practice of Gleiss Lutz. Eike advises national and international clients on corporate law and compliance. He is a specialist in strategic compliance advisory and compliance investigations. He has particular expertise in corporate governance issues, board matters and company group law issues.

Eike studied at the universities of Saarbrücken, Freiburg and Cambridge (LLM 2005). He has been with Gleiss Lutz since 2015. Eike was previously a partner at a prestigious compliance boutique firm in Frankfurt. In 2014, Eike took up a lectureship in compliance at the University of Bayreuth. Eike speaks German and English.

Caroline Black
Dechert LLP

Caroline Black is at the forefront of the corporate investigations field, acting as trusted adviser for over a decade to companies and individuals involved in the world's largest and most complex cases. She is a criminal defence lawyer and advises organisations, boards and audit committees on conducting investigations and interacting with relevant national authorities, including the Serious Fraud Office, HM Revenue and Customs and the police (and their overseas equivalents). Ms Black focuses her practice on the investigation and defence of business crimes, particularly matters involving corruption, money laundering, fraud and tax concerns.

She has received awards for training and management and has been recognised by *Global Investigations Review* as part of its 'Women in Investigations' issue, which highlighted 100 remarkable women in this field of law from around the world. *Who's Who Legal: Investigations* 2019 has recognised her as a Future Leader, with clients stating that she is 'impressive in her clear-thinking approach to solving important issues'. Ms Black is described as having 'the ability to keep cool in complex and stressful situations' in *The Legal 500 UK* 2018 and is acknowledged by Euromoney's *Expert Guides* 2019 as an Expert for White Collar Crime in the United Kingdom.

Todd Blanche
Cadwalader, Wickersham & Taft LLP

Todd Blanche is a partner in the white-collar defence and investigations group at Cadwalader, Wickersham & Taft LLP. He served for nearly a decade as an Assistant US Attorney for the Southern District of New York. As co-chief of the White Plains Division, he supervised investigations and prosecutions involving public corruption, securities fraud, bank and wire frauds, Medicare and federal programme frauds, RICO violations, violent crimes, and other criminal violations. He also served as co-chief of the Violent Crimes Unit. Todd has extensive trial experience, serving as counsel in 15 federal jury trials. Todd is a recipient of

the Director's Award from the US Department of Justice for Superior Performance as an Assistant US Attorney.

Todd received his undergraduate degree in political science and interdisciplinary studies from American University, and his law degree, *cum laude*, from Brooklyn Law School, where he was the editor of the *Brooklyn Law Review*. He held clerkships with the Hon. Joseph F Bianco for the US District Court for the Eastern District of New York and the Hon. Denny Chin of the US District Court for the Southern District of New York (both now judges of the US Court of Appeals for the Second Circuit).

Bradley J Bolerjack
Reed Smith LLP

Bradley J Bolerjack is a partner in Reed Smith's global regulatory enforcement group in Chicago, where he focuses on complex criminal law matters including sensitive internal investigations, grand jury investigations, compliance counselling and trial practice. Recent engagements have included investigations or indictments (or both) relating to the Foreign Corrupt Practices Act, commercial bribery, antitrust cartels, healthcare fraud, tax evasion, white-collar fraud and government contracting fraud. Brad has been notably successful in avoiding indictment of numerous high-profile clients even after they have received target status. In cases that are indicted, Brad has obtained outstanding results for many clients, whether through trial or negotiated resolutions. His clients include consumer product, medical device, pharmaceutical, manufacturing and other domestic and international companies, as well as individuals.

Nicolas Bourtin
Sullivan & Cromwell LLP

Nicolas Bourtin is a litigation partner and the managing partner of Sullivan & Cromwell's (S&C) criminal defence and investigations group. His practice focuses on white-collar criminal defence and internal investigations, regulatory enforcement matters, and securities and complex civil litigation. He is one of the coordinators of S&C's FCPA and anti-corruption practice group.

Mr Bourtin has represented individuals, corporations and financial institutions in numerous high-profile matters involving accounting fraud, antitrust, FIRREA, the FCPA, insider trading, money laundering, mortgage orientation and servicing, OFAC sanctions, securities fraud, tax fraud and trading. He has extensive experience in representing financial institutions in parallel regulatory and criminal investigations and representing non-US companies and individuals in connection with US investigations.

Mr Bourtin has conducted numerous jury trials and has argued frequently before the US Court of Appeals for the Second Circuit.

He is frequently recognised as a leading practitioner in the area of white-collar criminal defence.

Mr Bourtin also serves, *pro bono*, on the Criminal Justice Act panel for the Eastern District of New York, representing indigent defendants in federal criminal proceedings.

Mr Bourtin served for four years as an Assistant US Attorney in the Eastern District of New York, where he was involved in investigations, prosecutions and trials involving fraud, corruption, money laundering and other white-collar offences.

Michael Bowes QC
Outer Temple Chambers

Michael Bowes QC specialises in business crime, corruption, civil fraud, financial services and economic sanctions. He acts for corporate clients and senior managers in global investigations and for the SFO, FCA, CMA and Lloyd's of London. He advises companies in respect of US and EU sanctions. He acts for overseas regulators and is instructed in overseas cases as an expert in English law. He is regarded as an expert in civil and criminal 'cross-over' work and is described as 'one of the few specialist criminal practitioners in this area' (*The Legal 500* 2015) and as '[v]ery clever and has wide expertise, so is comfortable with criminal and civil work' (Financial Crime: Corporates, *Chambers 2017*). He is listed as a leading silk in the fields of financial services, financial crime (corporates) and financial crime (London) in *Chambers 2017*, and for banking and finance, business and regulatory crime, and fraud in *The Legal 500*. He is listed in *Who's Who Legal 2016* as an expert in business crime defence. He is a joint head of Outer Temple Chambers. He sits as a Deputy High Court Judge (Queen's Bench Division) and as a Recorder of the Crown Court. He is a Bencher of the Honourable Society of the Middle Temple. He is a trustee of Transparency International UK and a co-chair of the UK Chapter of the International Section of the New York State Bar Association.

Matthew Bruce
Freshfields Bruckhaus Deringer

Matthew Bruce is co-head of Freshfields' global investigations group in London, a member of the corporate crime group and an experienced commercial litigator. Highlighted as one of the world's 40 leading investigations specialists under the age of 40 by GIR and recommended by directories (including being listed as a leading investigations and/or litigation lawyer in *Chambers*, *Who's Who Legal* and *The Legal 500*), Matthew has led a number of major corporate internal and external investigations for blue-chip clients in all sectors arising from allegations of bribery and corruption, fraud, misaccounting and human rights abuses. Recent matters have engaged Asia, the Middle East, former CIS territories and Africa. Matthew has been a partner since 2012.

John D Buretta
Cravath, Swaine & Moore LLP

John D Buretta is a partner in Cravath's litigation department and a former senior official at the US Department of Justice (DOJ). He has represented global companies, boards of directors, audit committees, senior management and general counsels of public and private companies, law firms, and former US and foreign government officials with respect to internal investigations, criminal defence, regulatory compliance and related civil litigation matters. He has handled matters involving the Foreign Corrupt Practices Act (FCPA), anti-trust laws, securities fraud and disclosure regulations, money laundering and anti-money laundering controls, trade sanctions, export controls, cyber intrusion and tax compliance, and has appeared for clients before numerous US enforcement agencies. Mr Buretta served for 11 years in the DOJ, including supervising the Criminal Division, where he oversaw nearly 600 prosecutors in international investigative matters involving corporate fraud, the FCPA, insider trading, healthcare fraud, money laundering, the Bank Secrecy Act, trade

sanctions, asset forfeiture, cybercrime, intellectual property theft and public corruption. He currently serves as an independent monitor in separate appointments by the DOJ and US Department of Transportation.

Matthew Burn
Ropes & Gray LLP

Matthew Burn is a member of Ropes & Gray's litigation and enforcement practice group, based in London. Matthew's practice focuses on corporate and financial crime defence, contentious regulatory matters and internal investigations. Matthew has extensive experience advising both corporations and individuals facing complex cross-border investigations and prosecutions relating to allegations of bribery and corruption, money laundering, fraud and other types of misconduct or regulatory failings.

Matthew was previously seconded to a global financial institution and a leading professional services firm to assist with internal and regulatory investigations.

Matthew joined Ropes & Gray in 2018 from a magic circle firm in London.

Diego Cardona
Philippi Prietocarrizosa Ferrero DU & Uría – PPU

Diego Cardona is a partner at PPU and an expert in antitrust, unfair competition and consumer protection law. He has advised important clients in complex merger control procedures and has acted in some of the most important competition cases in Colombia. He has also participated in many administrative procedures and judicial actions regarding antitrust law, unfair competition and international trade. He was recently designated by the Colombian competition authority as non-governmental adviser for the International Competition Network.

James Carlton
Fox Williams LLP

James Carlton is a partner at Fox Williams LLP specialising in all areas of business crime and regulation. Sources say he 'inspires total confidence from his clients, has a wonderful knack of making them feel comfortable and superbly represented, while not pulling any punches in terms of problems they may face' (*Chambers*, 2017).

James has been instructed in a number of the largest and most complex white-collar investigations and prosecutions brought by the UK regulatory and prosecuting authorities, including the Serious Fraud Office and the Financial Conduct Authority, relating to, among other things, allegations of fraud, money laundering, insider dealing, market abuse, and bribery and corruption. Increasingly these have significant international dimensions and considerations.

James also has great expertise in the conduct of public inquiries. He has been instructed by interested parties in a large number of the highest-profile public inquiries, including, among others, the BSE, *The Marchioness*, Leveson, Pollard and Victoria Climbié inquiries.

He has been instructed on a number of complex and cross-border regulatory investigations for senior executives. He has also been instructed in relation to the regulatory investigations into the manipulation of LIBOR, EURIBOR and FX. He has extensive experience of

high-profile corporate investigations involving complex issues of financial crime, bribery and corruption, employee fraud and significant acts of dishonesty.

Sinead Casey
Linklaters LLP

Sinead Casey is a partner in Linklaters' employment and incentives group in London. She advises on a broad range of employment advisory and regulatory issues, including executive appointments and terminations, internal and regulatory investigations, group reorganisations and restructurings, outsourcings and the employment aspects of public and private M&A deals. She has particular expertise working with clients on crisis management mandates, advising them on their most challenging and sensitive HR-related issues as they navigate their way through a crisis.

Sinead's typical advisory work includes counselling on recruitment and termination, redundancy exercises, employment contracts, policies and procedures, grievance and disciplinary proceedings, the implementation of pension and other benefit changes, trade disputes and corporate governance-related issues.

Sinead represents clients before employment tribunals, the High Court and the Court of Appeal, including in unfair dismissal, discrimination and breach of contract claims.

Sinead has a special interest in diversity and is involved in Linklaters' graduate recruitment programme and various corporate social responsibility programmes.

Lavanyaa Chopra
Law Firm of Panag and Babu

Lavanyaa Chopra is part of Panag and Babu's internationally acclaimed compliance and investigations practice. Lavanyaa's advocacy is primarily focused on matters of financial fraud, bribery, money laundering and failure of internal control mechanisms.

Her experience includes conducting internal investigations into complex financial crimes and defending corporations facing multi-jurisdictional regulatory and law enforcement action.

Lavanyaa sectoral focus is principally financial institutions, which she helps in building robust internal controls and enhancing governance mechanisms.

Eric Christofferson
DLA Piper LLP

Eric Christofferson is an experienced litigation and compliance lawyer in DLA Piper's Boston office and is a member of the firm's white-collar group. He represents corporations and individuals in government investigations, internal investigations, criminal and regulatory proceedings, and civil litigation. Prior to joining DLA Piper, Eric served as an Assistant US Attorney in the District of Massachusetts, primarily prosecuting economic and other white-collar crime. Eric, whose practice focuses on the life sciences and financial services sectors, is an experienced courtroom lawyer who has tried more than 15 criminal and civil jury trials during his career.

Jonathan Cotton
Slaughter and May

Jonathan Cotton is a partner in Slaughter and May's dispute resolution group. He covers a range of cases involving contractual disputes, competition disputes and restructuring and insolvency matters. He also often advises on contentious aspects of corporate transactions, including takeovers.

He is particularly experienced in matters involving allegations of wrongdoing in its various forms. On the civil side, these have included cases involving the 'theft' of confidential information by employees and competitors, conspiracy and civil fraud. On the criminal and regulatory side, he has been involved in investigations and criminal prosecutions, cases concerning cartels, and regulatory cases concerning the Bribery Act, the Proceeds of Crime Act, the Fraud Act, FSMA, export controls and sanctions, and Companies Act offences.

The major investigations and disputes on which he has been engaged span business sectors including telecoms, investment banking, investment management, technology, heavy manufacturing, natural resources and fast-moving consumer goods.

Mark Chu
Herbert Smith Freehills

Mark Chu advises Chinese state-owned enterprises and private enterprises, and multinational corporations operating in China, on contentious matters. His practice focuses on compliance and investigations, international arbitration and US litigation. Mark is qualified in Illinois, United States, and Hong Kong. He is a native speaker of English and is fluent in Mandarin, and is based in Beijing.

Edward Craven
Matrix Chambers

Edward Craven is a barrister with particular expertise in media, criminal and data protection law. He is recommended by *The Legal 500* (2020) as a leading barrister in eight practice areas: media and entertainment; defamation and privacy; data protection; civil liberties and human rights; administrative and public law; environmental law; proceeds of crime; and public international law. He has extensive experience of advising individuals and corporations on a wide range of issues relating to business crime investigations and prosecutions, extradition and mutual legal assistance, reporting restrictions and related reputation management issues.

Gail E Crawford
Latham & Watkins

Gail Crawford is a partner in the London office and chair of the firm's data privacy committee and the global technology transactions practice. Ms Crawford is ranked as a leading individual for data protection privacy cybersecurity by *The Legal 500* (2019). Her practice focuses on advising on data protection, e-commerce and consumer protection legislation, as well as advising on technology, intellectual property and commercial law, including technology and intellectual property licensing agreements, joint ventures, technology procurement and outsourcing.

Ms Crawford is an editor of the Latham & Watkins Global Privacy & Security Compliance Law Blog and General Data Protection Regulation (GDPR) Resource Center.

Tracey Cui
Herbert Smith Freehills

Tracey Cui advises multinational and regional corporates operating in China on investigations and compliance matters, commercial dispute resolution and international arbitration. She has a particular focus on investigations and compliance issues that arise under PRC criminal law and anti-unfair competition law. Tracey has spent time on secondment at multinational corporates advising on anti-corruption investigations and compliance matters.

Tracey has passed the PRC National Bar Exam in 2009. She is fluent in Mandarin and English, and is based in Shanghai.

Christine Cuthbert
Herbert Smith Freehills

Christine Cuthbert is a senior associate in the Hong Kong disputes practice, specialising in corporate crime and investigations. She has extensive experience in all forms of contentious work, including cross-border investigations and litigation, and other corruption-related matters. Christine has been with Herbert Smith Freehills for more than 10 years and has worked in their offices in both Hong Kong and Australia. Her experience includes assisting clients with investigations by local and foreign authorities, internal investigations and corporate compliance, addressing anti-money laundering issues and dealing with other regulatory and enforcement bodies.

Christine is qualified to practise in Hong Kong and Australia (Queensland).

Robert Dalling
Jenner & Block London LLP

Robert Dalling is special counsel in Jenner & Block's investigations, compliance and defence practice group. Previously a criminal barrister, Robert has substantial experience in advising both individuals and corporates on issues including bribery and corruption, money laundering, fraud, benchmark manipulation (including LIBOR and FX), and trade and financial sanctions. As a result of the international nature of his caseload, he has acquired experience of a wide range of regulatory agencies operating within the UK (including the SFO, FCA and PRA), the European Union, the United States, Asia and elsewhere.

Eleanor Davison
Fountain Court Chambers

Eleanor Davison is a barrister at Fountain Court Chambers specialising in cross-border white-collar crime, fraud, corruption and contentious regulatory cases. Consistently recognised as expert in the fields of financial crime, financial crime (corporates), financial services and money laundering, by *The Legal 500* and *Chambers and Partners*, she has recently been described as having 'a phenomenal brain and in-depth knowledge of her area of expertise. She is quick-witted, alert to opposing arguments and a delight to work with – a real star to watch'

(*Chambers and Partners UK* 2019, Financial Crime). The directories also describe her as '[v]ery good and particularly experienced in complex investigations involving financial institutions'. Eleanor was listed in *Who's Who Legal* as a Future Leader in investigations in 2018.

Caroline Day
Kingsley Napley LLP

Caroline Day specialises in serious fraud and financial crime. She represents corporates and individuals in complex global investigations. She has conducted numerous internal investigations on behalf of companies in relation to allegations of financial crime and misconduct, including fraud, theft, corruption, money laundering and environmental crime. She advises companies and individuals who are subject to investigations and prosecutions by various agencies including the Serious Fraud Office, the Financial Conduct Authority, HM Revenue and Customs, the Crown Prosecution Service, and the Competition and Markets Authority. Caroline has a particular interest in cross-border cases and her experience extends to MLA requests and extradition. Caroline has been recognised in GIR's 100 'Women in Investigations 2018', and sits on the executive committee of the Fraud Lawyers Association.

Tapan Debnath
Nokia Corporation

Tapan Debnath is senior legal counsel for Nokia handling ethics and compliance investigations in Europe, the Middle East and Africa and serves as the compliance lead for the Nokia Enterprise Business Group. Prior to joining Nokia in January 2016, Tapan was a prosecutor at the UK's Serious Fraud Office, where he investigated and prosecuted major international economic crime cases. Tapan is an experienced English-qualified solicitor specialising in corporate crime and holds a certificate in financial crime from the University of London.

Rebecca Devaney
Pinsent Masons LLP

Rebecca Devaney is a solicitor at Pinsent Masons LLP and a member of the international white-collar crime, investigation and compliance team. She specialises in the conduct of investigations, self-reporting and anti-bribery compliance, as well as sanctions and export controls.

William H Devaney
Baker McKenzie LLP

William (Widge) Devaney is a partner in Baker McKenzie's North America litigation group in New York, co-chair of the firm's global compliance and investigations group and co-chair of the North American government enforcement practice. He was an Assistant United States Attorney in the District of New Jersey, where he was a member of the Securities Fraud Unit. Widge's main areas of practice are white-collar criminal defence, investigations, compliance and complex civil litigation.

Widge is the author of multiple publications involving such topics as the FCPA, investigations and corporate compliance programmes. He appears often in the print media commenting on current criminal matters.

Widge received an AB and JD from Georgetown University, and an LLM from Cambridge University. He clerked for the Hon. Oliver Gasch on the US District Court for the District of Columbia. He is a member of the New York Bar.

Enrico Di Fiorino
Fornari e Associati

Enrico Di Fiorino is a partner of Fornari e Associati, where he specialises in white-collar crime (serious fraud, tax evasion, bankruptcy, corporate crimes, market abuse) as a criminal defence counsel. He has particular expertise in environmental offences, anti-money laundering and medical malpractice.

Enrico advises companies and individuals in criminal inquiries and represents them in criminal proceedings. He has dealt with cases of criminal, internal and regulatory investigations, as well as representing clients in extradition proceedings and European arrest warrant cases.

Enrico is the author of various publications on environmental criminal law, tax law and corporate law. He frequently participates as a speaker in conferences on criminal law for executives, lawyers and accountants. He is a member of the European Criminal Bar Association, European Fraud and Compliance Lawyers, Extradition Lawyers' Association and International Bar Association.

J Robert Duncan
Cadwalader, Wickersham & Taft LLP

Robert Duncan, an associate in Cadwalader's white-collar defence and investigations group, advises clients in a variety of criminal, civil and regulatory matters, including compliance with the Foreign Corrupt Practices Act, and accounting and reporting regulations.

Prior to law school, Robert was a senior audit, assurance and risk advisory associate at a Big Four accounting firm. He is a licensed certified public accountant in the Commonwealth of Kentucky. Robert has taught undergraduate courses in accounting and auditing at the McIntire School of Commerce at the University of Virginia, where he has been a visiting lecturer and instructor.

Robert received his JD from the University of Virginia, where he served as a senior editor for the *Virginia Law and Business Review*. He earned his MS in accounting from the McIntire School of Commerce at the University of Virginia and his BS in accounting from Ball State University's Honors College. Robert is admitted to practise in the State of New York and the District of Columbia.

Kylie Dunn
Russell McVeagh

Kylie Dunn leads Russell McVeagh's national employment law practice. She routinely deals with regulatory and internal investigations, including providing advice on data protection, employment law and search orders.

Ciara Dunny
Matheson

Ciara Dunny is a senior associate in the regulatory and investigations team within the commercial litigation and dispute resolution practice. She has more than five years' experience in corporate crime and investigations and regularly advises both domestic and international clients on bribery, corruption, fraud, money laundering, investigations and trade sanctions, and related compliance issues. Ciara joined the team in July 2018 from Addleshaw Goddard's London office. Ciara's experience in investigations extends to the United Kingdom, the United States, Europe, China, Korea, the United Arab Emirates and Iran. Ciara also represents clients in large-scale civil litigation, including in relation to civil fraud, product liability, professional negligence and debt recovery. Ciara is recognised as being Most Highly Regarded in Europe in *Who's Who Legal: Investigations – Future Leaders* 2018 and 2019. She is also the only Irish lawyer listed in the Expert Guides *Rising Stars* 2019 in white-collar crime and was shortlisted for Rising Star in Litigation in the Euromoney for Women in Business Law Awards Europe 2019.

Clémentine Duverne
Navacelle

Clémentine Duverne represents foreign and domestic clients. Prior to joining Navacelle, Ms Duverne worked in the white-collar department of a major US law firm.

During the past few years, Ms Duverne has represented clients in OFAC investigations of global institutions based in the European Union conducted by the US Department of Justice, New York County District Attorney's Office, New York State Department of Financial Services, Federal Reserve Bank of New York and Southern District of US Attorney's Office; foreign and domestic financial institutions before French criminal courts in fraud and counterfeiting matters; and individuals of a foreign subsidiary of a French institution in connection with a criminal investigation on charges of money laundering and tax evasion.

Allison Eisen
Cravath, Swaine & Moore LLP

Allison Eisen is an associate in Cravath's litigation department.

Jaime Orloff Feeney
Ropes & Gray LLP

Jaime Orloff Feeney, an associate at Ropes & Gray in Chicago, frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Felipe Noronha Ferenzini
Trench Rossi Watanabe

Felipe Noronha Ferenzini joined the firm in 2009. He has more than 12 years of practice in the field of compliance, administrative law and regulatory, assisting public and private clients in national and multi-jurisdictional operations. Currently, Felipe is a teacher on a postgraduate course on compliance at Ibmec in Rio de Janeiro. He is also an alumnus of the International Anticorruption Academy. Felipe is a certified fraud examiner under the Association of Certified Fraud Examiners. Felipe worked at the London and Mexico offices of Baker McKenzie in 2016–2017. He has experience in compliance, leading complex investigations, implementation of compliance programmes, conducting risk assessment and training. He was one of the coordinators of the independent investigation at Petrobras in connection with Operation Car Wash. He also has significant experience in assisting clients in public procurements, negotiating contracts (including with the government), litigating and liaising with auditing authorities.

Kaitlyn Ferguson
Clifford Chance US LLP

Kaitlyn Ferguson represents clients in white-collar and government investigations and regulatory proceedings, with experience handling anti-fraud, anti-corruption/FCPA and anti-money laundering matters. She has represented clients facing scrutiny from the Department of Justice, Securities and Exchange Commission, and Commodity Futures Trading Commission, and has designed and conducted confidential internal investigations spanning multiple jurisdictions.

Reto Ferrari-Visca
Homburger

Reto Ferrari-Visca is an associate of Homburger's white collar and investigations team and litigation and arbitration practice. He specialises in domestic and international litigation and administrative proceedings. He has broad experience in internal and regulatory investigations and advises corporate clients in regulatory and compliance matters. His practice also focuses on privacy and data protection law and he regularly advises clients on cross-border privacy and data protection issues.

Rod Fletcher
Herbert Smith Freehills LLP

Rod Fletcher practised for more than 30 years in all aspects of white-collar and business crime. He represented both corporate and individual clients under investigation by regulators and prosecutors in many jurisdictions, including the Serious Fraud Office, the Financial Conduct Authority, the Department of Justice, the Securities and Exchange Commission, the Crown Prosecution Service and Her Majesty's Revenue and Customs. His work often involved assisting clients with internal corporate investigations.

Rod led the team advising ICBC Standard Bank plc in relation to the ground-breaking first-ever deferred prosecution agreement entered into in the United Kingdom. The case was

also the first disposal in England of the new corporate offence of failure to prevent bribery under the Bribery Act 2010, and involved a co-ordinated global settlement involving the US Department of Justice and the Securities and Exchange Commission. The case had no precedent and set the template for DPAs in the United Kingdom.

Rod also acted in the global LIBOR and FX investigations, and had extensive experience in cartel investigations and prosecutions, including appellate proceedings in the Supreme Court. He represented clients in the SFO investigations into Rolls-Royce, GSK and Tesco, and a defendant in the SFO prosecution arising from the raising of capital by Barclays Bank from Qatar in 2008.

He passed away in November 2019, after a period of illness.

Jonathan Flynn
BCL Solicitors LLP

Jonathan Flynn is an employed barrister specialising in criminal and regulatory law. He has particular expertise in fraud, bribery and corruption, restraint and confiscation proceedings, and general crime.

Jonathan has acted in a number of high-profile, complex and multi-jurisdictional cases, including investigations or prosecutions by the CPS, the FCA, HMRC, the SFO and the NCA.

Lisa Foley
Dechert LLP

Lisa Foley focuses her practice on white-collar crime and has particular experience in the investigation and defence of matters involving international fraud, money laundering and corruption.

Ms Foley advises organisations and individuals on internal investigations, multi-jurisdictional regulatory investigations, raids and prosecutions undertaken by authorities and regulators such as the Serious Fraud Office, the National Crime Agency and the Financial Conduct Authority.

Héctor Gadea
Rebaza, Alcázar & De Las Casas

Héctor Gadea is a graduate lawyer from the Pontifical Catholic University of Peru. In 2014, he was awarded an LLM by Columbia University, New York. In addition, he holds a master's degree from the universities of Barcelona and Pompeu Fabra (Spain). Héctor is certified by the Society of Corporate Compliance and Ethics as a compliance and ethics professional.

Héctor is a partner at the firm, where he focuses his practice on litigation, white-collar crime and corporate compliance. He is a former criminal law lecturer at the Pontifical Catholic University and the Peruvian Judiciary Academy. He has participated as a speaker at a number of international conferences and events.

João Augusto Gameiro
Trench Rossi Watanabe

João Augusto Gameiro became partner of the firm in 2018. He has more than a decade of experience in criminal law and compliance. As a criminal lawyer, he has represented several multinational companies and their shareholders and directors in police inquiries, criminal proceedings, administrative proceedings and parliamentary committees of inquiry in cases of tax evasion, environmental crimes, consumer crimes, antitrust, corruption, trademark and patent infringement, unfair competition, money laundering and currency evasion. He has also provided legal advice to foreign companies regarding Brazilian criminal law, participated in due diligence projects focused on criminal liability and exposure to anti-corruption and anti-money laundering legislation, and has conducted internal investigations into corporate fraud and competitive violations.

Mr Gameiro holds a law degree (2003) and a master's degree in criminal law (2007) from the University of São Paulo and a postgraduate degree in economic criminal law (2014) from the University of Coimbra. He attended the intensive corporate compliance and ethics course at New York University in 2015.

Sona Ganatra
Fox Williams LLP

Sona Ganatra is a partner at Fox Williams LLP specialising in financial services regulatory investigations and internal investigations. She has extensive experience in advising corporates and individuals on a broad range of regulatory issues, particularly in relation to financial crime (such as money laundering, bribery and corruption, and fraud) as well as issues arising in relation to consumer-credit activities, payment services and e-money. She is regularly instructed in relation to FCA and SFO investigations, prosecutions and enforcement action against corporates and senior individuals. She also has extensive experience of high-profile corporate investigations advising on issues of self reporting to and liaising with a variety of regulatory bodies and prosecuting authorities.

Earlier in her career, Sona was seconded to the Enforcement Division of the Financial Services Authority, where she appeared before the Regulatory Decisions Committee and participated in settlement discussions with financial institutions. This provided her with invaluable insight into regulatory investigations and disciplinary actions.

Sources describe Sona as understanding 'the commercial realities and personal pressures of investigations and proceedings and help[ing] clients manage both' (*The Legal 500*, 2019) and as 'an expert on UK banking regulation' who regularly represents senior executives who are subject to regulatory investigations (*The Legal 500*, 2017).

Tanya Ganguli
Law Firm of Panag and Babu

Tanya Ganguli is part of Panag and Babu's internationally acclaimed compliance and investigations practice. Tanya's advocacy is primarily focused on matters of bribery, corporate governance enhancement and failure of internal control mechanisms.

The core of Tanya's practice is advising multinational companies on matters involving the violation of Indian anti-corruption laws and their interplay with the US Foreign Corrupt

Practices Act, Germany's Criminal Code, the UK Bribery Act, and other foreign legislation dealing with bribery of foreign public officials in India.

Tanya's sectoral focus is manufacturing companies, which she helps in building robust internal controls and enhancing governance mechanisms.

Courtney A Gans
Cravath, Swaine & Moore LLP

Courtney A Gans is an associate in Cravath's litigation department.

Jacob Gardener
Walden Macht & Haran LLP

Jake is an experienced litigator who represents corporations and individuals in criminal, civil and regulatory matters. He has extensive experience managing internal and government investigations, complex commercial disputes, and appeals. He has helped lead internal investigations into high-stakes matters involving alleged violations of the FCPA and securities laws. Jake has also successfully handled numerous civil cases in a variety of areas, including commercial contract disputes, mortgage-backed securities litigation, shareholder derivative actions, bankruptcy and employment law. He has significant courtroom experience, including briefing and arguing several appeals and dispositive motions in criminal and civil cases. Before joining Walden Macht & Haran, Jake clerked for the Hon. Dennis Jacobs of the US Court of Appeals for the Second Circuit and the Hon. Naomi Reice Buchwald of the US District Court for the Southern District of New York. In addition, Jake served for several years as a New York City firefighter. His academic scholarship has been published in the *Journal of Criminal Law and Criminology* and the *Boston University Journal of Science and Technology Law*. Jake is a graduate of Yale Law School and Stanford University.

Laura Gillespie
Pinsent Masons LLP

Laura Gillespie is a partner, qualified in Northern Ireland. Laura has more than 15 years' experience in the jurisdiction. She has particular experience in internal investigations and has been involved in a range of international investigations. Laura also handles civil fraud, complementing her investigation experience. She also regularly helps clients with board-level training and policy implementation.

Hector Gonzalez
Dechert LLP

Hector Gonzalez, the chair of Dechert's global litigation practice and a member of the firm's policy committee, is a Fellow in the American College of Trial Lawyers. He advises corporations and executives on a wide range of matters, with a focus on complex commercial and securities litigation, criminal and related civil and administrative matters, SEC and CFTC enforcement proceedings, and internal, grand jury and state attorneys general investigations. In addition, he regularly represents clients in all aspects of Foreign Corrupt Practices Act (FCPA) matters and has extensive experience in working on matters in Latin America.

Mr Gonzalez has been consistently recognised for his white-collar criminal defence and litigation practices by *The Legal 500: United States*, which praises him as 'a great lawyer', having 'an extraordinary amount of expertise' in securities shareholder litigation, and being 'an excellent trial lawyer and strategic thinker who won't waste clients' time or money'. *Benchmark Litigation* named Mr Gonzalez a Litigation Star for his white-collar defence practice and described him as 'one of the sharpest and most promising talents doing this work right now'. He is also ranked in *The Best Lawyers in America* for his white-collar criminal defence practice.

Mr Gonzalez has significant trial experience, having tried more than 20 federal and state jury trials and argued more than 30 cases before federal and state appellate courts. He was previously an Assistant US Attorney in the US Attorney's Office for the Southern District of New York, where he served as Chief of the Narcotics Unit and was twice awarded the Department of Justice's Director's Award for Superior Performance.

Lara Gotti
Clifford Chance

Lara Gotti is a senior associate in Clifford Chance's litigation and dispute resolution practice based in Perth. Since joining Clifford Chance, Lara has worked predominantly on white-collar and regulatory enforcement matters, with a focus on disputes and clients in the energy and resources sector.

Lara has experience in advising corporations, individuals and boards on regulatory investigations and corporate governance issues such as insider trading, bribery and corruption, tax fraud, misleading and deceptive conduct, unconscionable conduct, false and misleading representations, continuous disclosure, anti-corruption and market manipulation.

Tim Grave
Clifford Chance

Tim Grave specialises in regulatory investigations, commercial dispute resolution and related advice across a wide range of matters, including Corporations Act matters, directors' duties, commercial and contractual disputes, equitable claims, white-collar crime, competition law, sanctions advice, internal investigations and contentious enforcement matters. His experience includes acting for global banks, directors and officers of listed companies, and employees on regulatory investigations. Some recent examples of Tim's experience include acting for the former chairman of an Australian listed entity in ongoing investigations by the Australian Securities and Investments Commission (ASIC) in relation to allegations of foreign bribery; for a director of a publicly listed company in an investigation by ASIC concerning allegations of insider trading; for a company director in a high-profile criminal prosecution for alleged conspiracy to commit insider trading offences; for the chief financial officer of an Australian listed entity in a corruption inquiry; for a global transport company on an internal investigation; for the chief executive officer and managing director of a Forex/contracts for difference provider in an ASIC investigation and related proceedings; and in multiple class actions.

Kelly Hagedorn
Jenner & Block London LLP

Kelly Hagedorn is a partner in Jenner & Block's investigations, compliance and defence practice group. Kelly focuses her practice on white-collar crime, data privacy matters (including data breaches), and international disputes involving fraud allegations. She has particular expertise in matters involving the financial services, gaming, hospitality and outsourcing sectors.

In 2018, Kelly was named in *Global Data Review*'s inaugural '40 under 40' list of up-and-coming professionals working in the field of data law.

Graeme Hamilton
Borden Ladner Gervais LLP

Graeme Hamilton is the national co-chair of BLG's investigations and white-collar defence group. Graeme maintains a trial and appellate practice encompassing commercial litigation, public law and white-collar criminal defence. Graeme has been lead counsel in dozens of trials and contested hearings. He also has substantial appellate experience in both criminal and civil matters. Graeme teaches trial advocacy at the University of Toronto Faculty of Law and previously taught evidence at Osgoode Hall Law School as an adjunct professor. Graeme is well-known to his clients for his strategic focus, exceptional problem-solving skills, entrepreneurial business sense and management skills that build trust and consensus. He has been repeatedly recognised as being at the top of his field by his peers in Benchmark Canada – The Definitive Guide to Canada's Leading Litigation Firms & Attorneys (Future Star), and he is recognised in the 2019 edition of Benchmark Canada 40 and Under Hotlist.

Graeme is a sought-after speaker and author. He has presented in a variety of venues and has published many articles and professional papers. He is called to the Ontario Bar.

John M Hillebrecht
DLA Piper LLP

John M Hillebrecht is the US national co-chair of DLA Piper's white collar, corporate crime and investigations practice. Immediately prior to joining DLA Piper in 2010, John served for 15 years as an Assistant United States Attorney in the Southern District of New York (SDNY), garnering extensive trial, appellate and supervisory experience.

He has served as lead or sole counsel in more than 20 jury trials and approximately 50 Second Circuit appeals. John has represented entities and individuals in the crosshairs of some of the highest-profile criminal investigations of recent years, including the 'expert network' insider trading cases, RMBS fraud prosecutions, the SDNY investigation regarding possible corruption in Governor Cuomo's 'Buffalo Billion' and related development projects, numerous rate-fixing cases (including the LIBOR, FX and ISDAfix manipulation cases), the GM ignition switch case, the ongoing Fiat Chrysler emissions control 'defeat device' investigation, and various FCPA investigations (including the 'Sons and Daughters' DOJ and SEC investigation into banks' hiring practices in China and an ongoing investigation involving one of the world's largest petroleum companies) and False Claims Act matters. He also regularly represents pharmaceutical and medical device companies and individuals in various kinds of investigations.

John is recommended in *The Legal 500 United States* and recognised in *The Best Lawyers in America*. In December 2015, *The National Law Journal* recognised John as one of the top white-collar practitioners in the country.

Louise Hodges
Kingsley Napley LLP

Louise Hodges is the head of the criminal department at Kingsley Napley LLP. She specialises in all fraud and business crime litigation, including investigations and prosecutions by the Financial Conduct Authority, the Serious Fraud Office (SFO), the National Crime Agency, HM Revenue and Customs, the City of London Police and the Crown Prosecution Services. She is head of the Kingsley Napley financial services group and lead partner in the internal investigations team. Louise has a particular interest in cross-border cases representing companies and individuals; in particular she is part of the team representing Tesco in the deferred prosecution agreement with the SFO. Louise is past chair of the Fraud Lawyers Association and former vice chair of the European Criminal Bar Association.

Eugene Ingoglia
Allen & Overy LLP

Gene Ingoglia is a partner in the investigations and litigation practice at Allen & Overy LLP based in New York. His practice focuses on criminal, civil and regulatory securities and anti-corruption matters as well as trial-ready civil litigation. He has extensive experience in handling sophisticated securities and business crime matters and has achieved notable results for a wide variety of clients. He has represented clients in actions and investigations by various US Attorney's Offices, the SEC, the CFTC, FERC, FINRA as well as other US federal and state regulatory agencies in actions and investigations involving allegations of securities fraud, accounting fraud, insider trading, market manipulation, FCPA violations, money laundering, tax evasion, and healthcare fraud.

Previously, Gene was an Assistant US Attorney for the Southern District of New York and a member of the Securities and Commodities Fraud Unit, serving as the lead attorney in numerous federal jury trials and complex white- collar investigations. In that position, he represented the government in the trial and conviction of former SAC Capital portfolio manager Mathew Martoma in the largest insider trading scheme ever charged; led the investigation in the so-called 'London Whale' case alleging the deliberate mismarking of complex securities in order to hide losses and resulting in charges against two former traders at a multinational financial institution; and led the investigation that resulted in the conviction of former bank executives and traders for deliberately overstating the value of certain real estate backed securities in *United States v. Kareem Serageldin*, one of the few successful criminal prosecutions arising out of the financial crisis.

Katrin Ivell
Homburger

Katrin Ivell is a partner of Homburger's white collar and investigations team and the financial services team. She specialises in internal investigations, including when the allegation

relates to sexual harassment or similar misconduct, and advises financial institutions in regulatory and compliance matters. She has conducted monitorships for the Swiss Financial Market Supervisory Authority (FINMA), advised several Swiss banks under the Swiss Bank Programme and is frequently retained by banks in anti-bribery and corruption and anti-money laundering issues.

Andrés Jana
Bofill Mir & Alvarez Jana

Andrés Jana is a founding partner at Chilean law firm Bofill Mir & Alvarez Jana, where he chairs the litigation and international disputes area. He obtained his LLM from Harvard University and graduated *summa cum laude* from the Law School of the University of Chile.

A professor of private law at the University of Chile since 1997, he regularly lectures and publishes on international disputes.

Stacy Keen
Pinsent Masons LLP

Stacy Keen is a specialist in white-collar and business crime. Stacy's areas of expertise include trade and financial sanctions, export controls, bribery, money laundering, and health and safety; in these areas she provides advice on all aspects of investigations, prosecutions, risk management and compliance. Stacy regularly advises oil and gas companies and advanced manufacturers on compliance with Russian and Iranian sanctions, on export controls and on responding to suspected violations of those laws, including the making of voluntary disclosures to HM Revenue and Customs and HM Treasury. She also specialises in compliance with bribery laws, on investigations stemming from corrupt activities and on corporate self-reporting.

Asena Aytuğ Keser
Gün + Partners

Asena Aytuğ Keser has been with the firm since 2011 and is a senior associate. Her practice focuses on dispute resolution, employment, business crime and anti-corruption.

Asena's main area of practice is commercial dispute resolution. She has a specific focus on business crimes and handles various disputes that require the application of both civil and criminal law principles. She advises and represents various multinational companies and their executives with regard to investigations and criminal actions arising from white-collar crimes.

Asena is also experienced in employment law. She provides consultancy and represents clients in relation to a wide range of employment law issues, including preparation and negotiation of employment contracts, personnel management, re-employment and unjust competition actions.

Combining her experience in business crimes and employment law, Asena actively takes part in internal investigation processes of major multinational companies from the beginning, and advises clients on the planning and conduct of the investigation.

Pamela Kiesselbach
Herbert Smith Freehills

Pamela Kiesselbach specialises in corporate crime and investigation matters, as well as disputes. She currently splits her time between Hong Kong and south-east Asia, where she leads teams on some of the largest, and most complex, cross-border internal investigations currently under way anywhere in the world.

She has more than 20 years' experience in assisting multinational and regional clients involved in high-value, cross-border investigations and disputes involving Asian, Australian, European, UK and US companies. Pamela has broad sector experience, spanning energy companies, international and regional investment banks and other financial services providers, transport companies, manufacturers and clients in the technology and telecommunications sectors.

Pamela speaks regularly at conferences in Hong Kong and Singapore and the wider Asia-Pacific region about topics relevant to anti-corruption, cybersecurity, anti-money laundering and corporate crime.

Michelle de Kluyver
Addleshaw Goddard LLP

Michelle de Kluyver is a partner in Addleshaw Goddard's global investigations and contentious regulatory group. Michelle has extensive experience in complex, cross-border financial crime investigations including bribery and corruption, financial sanctions, money laundering and fraud, and also advises clients on related compliance issues. Michelle is also an expert on directors' duties. Michelle is named as a Thought Leader in *Who's Who Legal Business Crime: Defence*. Michelle was selected by *Global Investigations Review* in 2015 as one of 100 remarkable women investigation specialists operating across the world. WWL says: 'Michelle receives widespread plaudits from international peers for her "fantastic" work on cross-border international investigations relating to fraud, bribery and corruption claims.' Michelle and co-author Ben Koehne contributed the chapter on Directors' Duties for the 6th Edition of Sweet & Maxwell's *A Practitioner's Guide to Directors' Duties and Responsibilities*.

Bettina Knoetzl
Knoetzl

Bettina Knoetzl, co-founding partner at KNOETZL, is a leading Austrian trial lawyer with 25 years' experience in Austrian and international high-stakes commercial litigation and business crime matters. She has been a partner in international law firms since 1999 and has tried and resolved hundreds of significant, complex disputes and won important business crime trials for her clients, often under significant media attention.

Bettina specialises in complex litigation, business crime, fraud and asset tracing, compliance and corporate crisis management. Her clients are corporations, multinationals and governments, as well as individuals under their company's protection; her matters usually have complex cross-border aspects. Bettina has been involved in a significant number of internal and external investigations, including investigations under the US Foreign Corrupt Practices Act carried out throughout central and eastern Europe.

For many years, she has been ranked in the top tier by leading international directories, including *Chambers* in litigation and white-collar crime (both Band 1) and is currently

recognised as one of the 10 Most Highly Regarded Individuals in litigation and asset tracing in Europe (*Who's Who Legal*, 2018). In 2017, she received recognition as international Lawyer of the Year in asset recovery (*Who's Who Legal*, 2017).

Bettina is very active in the International Bar Association, for which she chaired the Litigation Committee in 2016–2017. She is president of Transparency International – Austrian Chapter.

Anita Lam
Clifford Chance

Anita Lam is the head of employment, Hong Kong. Anita practises across all areas of employment law, with a particular focus on contentious employment, discrimination and data privacy disputes. As a seasoned litigator, Anita is one of very few solicitors in Hong Kong who has Higher Rights of Audience granted by the Higher Rights Assessment Board.

Sarah Lambert-Porter
Ropes & Gray LLP

Sarah Lambert-Porter is a senior associate in Ropes & Gray's litigation and enforcement practice group, based in London.

Sarah's practice focuses primarily on financial crime including bribery and corruption, terrorist financing, money laundering, fraud, and other misconduct and regulatory failings. She has substantial experience advising financial institutions in relation to internal investigations as well as complex cross-border contentious regulatory matters, and criminal investigations and prosecutions. Sarah also advises in relation to the UK's Senior Managers and Certification Regime.

Sarah was previously seconded to a global financial institution to assist with the design and implementation of controls in relation to the Senior Managers and Certification Regime.

Sarah joined Ropes & Gray in 2018 from a magic circle firm in London.

Margot Laporte
Miller & Chevalier Chartered

Margot Laporte advises global clients facing complex multi-jurisdictional regulatory, litigation, and reputational risk arising from enforcement matters. Her practice focuses on cross-border internal and regulatory investigations, white collar criminal defence, securities enforcement matters, and regulatory compliance, including with respect to the Foreign Corrupt Practices Act, anti-money laundering regulations, economic sanctions laws, insider trading, and accounting fraud. She has represented global public companies, boards of directors, audit committees, financial institutions, hedge funds and senior officers in enforcement matters before numerous US and foreign regulators, including the US Department of Justice, the US Securities and Exchange Commission and the Financial Industry Regulatory Authority, as well as France's Autorité des marchés financiers and other foreign regulators.

Nico Leslie
Fountain Court Chambers

Nico Leslie is a member of Fountain Court Chambers, London.

He was called to the Bar in 2010 and has since developed a practice involving both national and international disputes. In particular, he has done significant work in Singapore, both in arbitration and before the newly formed Singapore International Civil Court.

Nico's practice comprises mainly complex financial and civil fraud litigation, having acted in some of the largest UK disputes of recent years, including the *Sebastian Holdings*, *Algosaibi*, *Gemini* and *Republic of Djibouti* cases. In light of this experience, Nico was recently identified as one of 10 junior 'Stars at the Bar' by the UK legal press.

Nico is the co-author (with Marcus Smith QC) of *The Law of Assignment* (published by OUP), one of the leading texts on the creation and transfer of intangible property. He has also been commissioned by OUP (with Marcus Smith QC) to write a further book: *Private International Law and Intangible Property*. Nico speaks fluent French, Italian and Serbo-Croat, and is comfortable working in those languages.

Megan Y Lew
Cravath, Swaine & Moore LLP

Megan Y Lew is a practice area attorney in Cravath's litigation department. Her practice focuses on internal and government investigations, civil litigation and regulatory compliance, including matters concerning the FCPA, fraud, money laundering and anti-money laundering controls, trade sanctions and export controls.

Richard Lissack QC
Fountain Court Chambers

Richard Lissack QC is a member of Fountain Court Chambers, London.

He is currently and has been repeatedly recognised by all the directories and his peers as a leading practitioner across many disciplines and in particular the law of banking and financial services, regulation and compliance, and white-collar crime.

He was called to the Bar in 1978, and became a Queen's Counsel when aged just 37 in 1994. He is also a QC at the Bar of the Eastern Caribbean, and the Bar of Northern Ireland, and an FLC at the Bar of New York, and most recently became admitted with full rights of audience at the DIFC. He has for over 20 years sat as a judge and as an arbitrator.

His practice is national and international and is currently involved in litigation in London, New York, San Francisco, Abu Dhabi, Dubai, the British Virgin Islands and Switzerland.

His practice comprises mainly high-profile complex litigation and is heavily weighted towards points at which commercial conduct straddles the line between civil, regulatory and criminal law – and in particular cross-border work involving banking and the financial markets.

Richard is co-author of the leading book on the Bribery Act 2010 and also the only post-*Lehman* review of Financial Services regulation in the UK. Both are published by LexisNexis.

He is also consulting editor to OUP's *Public Inquiries*.

Gayle E Littleton
Jenner & Block LLP

Gayle Littleton is a partner at Jenner & Block and a member of its investigations, compliance and defence and litigation practices. She focuses on advising and defending corporations in connection with anti-corruption (FCPA), fraud, whistleblower complaints, #MeToo allegations and regulatory compliance matters; conducting complex, worldwide internal investigations; and defending corporations in connection with civil actions brought pursuant to the False Claims Act and the Financial Institutions Reform, Recovery and Enforcement Act. Before joining Jenner & Block, she served as a federal prosecutor for 12 years, working in the US Attorney's Offices for both the Northern District of Illinois and the Northern District of Florida. She served on the team that investigated and prosecuted former Illinois Governor George Ryan's chief of staff. She also investigated and prosecuted high-level white-collar cases and served as senior litigation counsel to the US attorney, where she advised on charging decisions. She graduated from Cornell Law School and served as a law clerk to the Hon. Joseph L Tauro of the US District Court for the District of Massachusetts and the Hon. Gerald W Heaney of the US Court of Appeals for the Eighth Circuit. She is admitted to practise in New York, Illinois and Florida.

Augusto Loli
Rebaza, Alcázar & De Las Casas

Augusto Loli is one of the main partners of Rebaza, Alcázar & De Las Casas, where he leads the litigation practice area. He has over 20 years of experience as a professional attorney specialising in white-collar crime, compliance and complex corporate litigation. He has designed and implemented the defence strategies of several high-profile criminal cases involving public officials, the financial sector, telecommunications infrastructure, industry and commerce for clients from Latin America, the United States and Europe. He graduated from the National University of San Marcos and completed his master's studies in criminal law at the same university. He is a professor of white-collar criminal law at the St Ignatius of Loyola University and of procedural criminal law at the University of Piura.

In addition to his private practice, he has been consulted several times by government entities, including the Advisory Committee of the Commission of Human Rights of the Congress of the Republic of Peru and the Citizen Security Commission. He is recognised by international legal publications as a leading lawyer and recommended in Peru as an expert within his field.

James P Loonam
Jones Day

James Loonam is a partner at Jones Day in New York City where he regularly advises companies and their senior executives in sensitive investigations. Prior to joining Jones Day, James was an Assistant US Attorney for the Eastern District of New York and Deputy Chief of that office's business and securities fraud section. James graduated from the University Connecticut School of Law with honours, where he was a member of the Law Review.

Rebecca Loveridge
Fountain Court Chambers

Rebecca Loveridge is a barrister practising from Fountain Court Chambers who specialises in all areas of commercial law, including civil and regulatory proceedings relating to financial services. She is regularly instructed on matters concerning privilege and appeared as junior counsel for the Bar Council in *R (on the application of Prudential and another) v. Special Commissioner of Income Tax and another* [2013] UKSC 1 and as junior counsel for ENRC in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2019] 1 WLR 791. She is also a contributor to the latest edition of *The Law of Privilege*, published by Oxford University Press.

Joanna Ludlam
Baker McKenzie LLP

Joanna Ludlam, a partner in the Baker McKenzie dispute resolution team based in London, leads the market-leading regulatory, public and media law team and co-chairs the firm's global compliance and investigations group.

Joanna advises clients in the areas of corporate investigations, administrative and public law, procurement law and litigation. She has particular expertise in the healthcare, technology and energy, mining and infrastructure sectors. Joanna handles all kinds of high court litigation as well as investigations, including issues of bribery, corruption and fraud. She advises clients, frequently at board level, on regulatory compliance and crisis and reputation management.

Joanna has been recognised by several industry directories and has won numerous awards for her work. She has been named one of *The Lawyer*'s Hot 100 for her practice, recognised by *Who's Who Legal* as a Future Leader of Legal Investigations and described as having an 'excellent reputation within the market', ranked by *Chambers and Partners* with commentators saying 'she is "excellent, knowledgeable and well connected"', and acknowledged by the *Financial Times* as a Champion of Women in the annual FT HERoes awards.

Ben Luscombe
Clifford Chance

Ben Luscombe leads the litigation and dispute resolution practice. He has close to 40 years' experience of representing parties in major arbitrations, major litigation, dispute resolution and advisory and regulatory investigations throughout Australia and Asia. Ben is continuously recognised in leading legal publications, such as *Chambers Global*, *The Legal 500 Asia Pacific* and *Best Lawyers Australia*.

Ben leads some of the highest-profile regulatory, international and domestic dispute cases in the region. In the regulatory space, he has experience in advising a variety of clients on domestic and cross-border regulatory investigations involving insider trading, misleading and deceptive conduct, continuous disclosure, anti-corruption, market manipulation and tax prosecutions.

Michael McGovern
Ropes & Gray LLP

Michael McGovern is co-head of Ropes & Gray's global government enforcement group, concentrating his practice in the areas of white-collar criminal defence and complex civil litigation, with a particular focus on investigations and prosecutions by the US Department of Justice and the Securities and Exchange Commission of alleged violations of the federal antitrust laws, the federal securities laws (including the Foreign Corrupt Practices Act), and alleged violations of various healthcare laws and regulations (including the False Claims Act). Michael has over 25 years of experience representing international and domestic corporations and partnerships, as well as officers, directors and other individual clients in complex criminal and civil investigations and litigation. Michael is listed in *The National Trial Lawyers* Top 100 Criminal Defense Trial Lawyers – New York, *Benchmark Litigation*, *Chambers Global*, *The Legal 500* and *The Best Lawyers in America*.

Prior to joining Ropes & Gray, Michael served for over seven years as an Assistant United States Attorney in the US Attorney's Office for the Southern District of New York, where he held supervisory positions in both the organised crime and terrorism unit and the general crimes unit.

Tara McGrath
Clifford Chance US LLP

Tara McGrath is an associate at Clifford Chance US LLP, where she represents clients in international and domestic white-collar government investigations, and related regulatory and civil proceedings. Her recent representations have involved allegations of securities and accounting fraud, wire fraud and money laundering, in addition to issues of extradition. Tara received her BA from Vassar College and her JD, *cum laude,* from Duke University School of Law.

Neil McInnes
Pinsent Masons LLP

Neil McInnes, partner and barrister, is a criminal defence specialist. He has extensive experience of conducting anti-corruption and related compliance advisory work for European, UK, Asia-Pacific and multinational corporates. He regularly advises clients on the implications of the UK Bribery Act and global anti-corruption trends, as well as on fraud, money laundering and related global regulatory investigations, frequently involving multiple law enforcement agencies around the world. He has been recognised as an expert for a number of years by *Who's Who Legal* in both the business crime corporate defence and investigations categories.

Claire McLeod
Barclays Bank PLC

Claire McLeod is the head of investigations and enforcement for Europe and the Middle East at Barclays. Prior to joining Barclays in 2013 Ms McLeod was at Simmons & Simmons LLP.

Claire McLoughlin
Matheson

Claire McLoughlin is a partner in the commercial litigation and dispute resolution department at Matheson and co-head of the firm's regulatory and investigations group.

Claire has advised a wide variety of clients on contentious matters, with a particular focus on the areas of financial services disputes, contractual disputes and corporate offences. Claire has also been involved in a number of judicial review proceedings, acting both for and against statutory bodies.

Claire is highly experienced in advising clients on all aspects of High Court, Commercial Court and Supreme Court litigation. The majority of Claire's cases consist of High Court and Commercial Court litigation matters. In this regard, Claire has developed experience in case management, disclosure and discovery requirements, including privilege and confidentiality issues, the instruction of experts and procedures relating to preliminary issues and modular trials. From a practical perspective, Claire has particular expertise in coordinating and managing large-scale discovery exercises.

Anthony M Mansfield
Allen & Overy LLP

Tony Mansfield focuses his practice on enforcement defence, civil litigation and regulatory advice involving commodities, securities and related financial derivatives. He regularly represents clients before US and European regulators including the Commodity Futures Trading Commission (CFTC), the Federal Trade Commission, the Federal Energy Regulatory Commission, other federal and state regulatory agencies, the UK Financial Conduct Authority and the European Commission. Tony works with a broad spectrum of market participants, including US and non-US financial institutions, major integrated oil companies, global trading companies, hedge funds, energy marketers, futures commission merchants and exchanges.

Prior to returning to private practice in 2007, Tony served as a chief trial attorney and counsel to the Director in the Division of Enforcement of the CFTC. While there, he managed a team of lawyers and investigators focused primarily on manipulation in the commodities markets. He was responsible for the Division's investigations of numerous energy and power marketing companies relating to price reporting in the natural gas markets. He also played a central role in the Commission's subpoena enforcement actions against natural gas price index compilers, involving First Amendment 'Reporter's Privilege' issues, and was central in the Commission's defence of its exercise of jurisdiction over false reporting in the natural gas markets pursuant to the Commodity Exchange Act.

Tony is a former member of the CFTC's energy and environmental advisory committee and the law and compliance executive committee of the Futures Industry Association.

Sergio Mattos
Rebaza, Alcázar & De Las Casas

Sergio Mattos is a graduate lawyer from the University of St Martin de Porres. In 2017, he was awarded a Chevening scholarship to complete a master of laws degree, with a particular emphasis on criminal justice, at the London School of Economics and Political Science (United Kingdom). He also holds a master's degree, with a specialisation in criminal law, from the University of Seville (Spain), where he also completed his doctoral studies in the same field.

Sergio is a senior associate at the Lima office, where he focuses his practice on litigation, white-collar crime and corporate compliance. He is a former lecturer in criminal law at the Scientific University of the South (Peru). He has also written and published several research articles focused on substantive aspects of criminal law, and he has been a speaker at a number of conferences, both in Peru and abroad.

Max G Mazzelli
Latham & Watkins

Max Mazzelli is an associate in the San Francisco office of Latham & Watkins. He is a member of the firm's litigation and trial department and practises in the area of data privacy, complex commercial litigation, consumer protection and cybersecurity.

Mr Mazzelli represents public and private technology companies in complex commercial and class action litigation in both state and federal courts involving data privacy, consumer protection, and commercial contract disputes. He represents companies in regulatory investigations and inquiries by the Federal Trade Commission (FTC), and other US and global government regulators, agencies and bodies. Mr Mazzelli also counsels technology clients on privacy and internet issues, in particular compliance with CCPA, FTC requirements, GDPR, TCPA, COPPA, BIPA, ECPA and wiretap issues, and CLOUD Act; behavioural advertising and social media; data collection; security incidents; and forensic investigations triggered by government requests for information. Additionally, he assists technology clients with privacy policy drafting and provides transactional support on privacy-related issues.

Francisca M Mok
Reed Smith LLP

Francisca Mok is the managing partner of Reed Smith's Century City office and a member of the global regulatory enforcement group. She represents companies and senior individuals in government investigations by criminal and civil authorities, such as the Department of Justice and Securities Exchange Commission, in cases involving the securities laws, Foreign Corrupt Practices Act and False Claims Act. She also regularly conducts internal investigations for clients in a variety of industries, including internal investigations of alleged violations of company policy and financial fraud, and investigations, pursuant to section 10A of the Exchange Act. Additionally, Francisca handles a variety of complex commercial litigation matters, including in the areas of securities law, unfair competition and class action litigation.

Gustavo Morales Oliver
Marval O'Farrell & Mairal

Gustavo Morales Oliver is a partner at Marval, O'Farrell & Mairal and has been a member of the firm since 2006. He specialises in compliance, anti-corruption and investigations.

He has advised companies from several industries on anti-corruption compliance issues and investigations relating to day-to-day company operations, mergers and acquisitions deals, compliance programmes, complex contracts and cases with the authorities.

Gustavo also has significant experience in corporate, mergers and acquisitions, litigation and cross-border matters.

Before joining the firm, he was in-house counsel in both the private and public sectors. Additionally, in 2010 he was a foreign attorney at Yuasa and Hara Law Firm in Tokyo, Japan.

Gustavo earned a law degree from the Torcuato Di Tella University College of Law in 2001, a specialist degree in finance from the University of San Andrés in 2009, and a master of laws degree (LLM) from the University of Illinois College of Law in 2010. In 2014, he earned the 'Leading Professional in Ethics and Compliance' certification granted by the Ethics and Compliance Officer Association ECOA (USA) and IAE Business School.

He teaches anti-corruption compliance and business law at the Torcuato Di Tella University College of Law. He has published numerous articles and is also a frequent speaker at local and international conferences.

Gustavo is co-director and co-author of the ebook *Tratado de Compliance*, published by Thomson Reuters. He is a member of the Bar of Buenos Aires and of the New York State Bar, and has been recognised by *Chambers Latin America* as a leading practitioner in his field.

Joseph Moreno
Cadwalader, Wickersham & Taft LLP

Joseph Moreno is a partner in the white-collar defence and investigations group at Cadwalader, Wickersham & Taft LLP. He has extensive trial and appellate experience in handling complex investigations and litigation involving the DOJ, the SEC, and other domestic and international law enforcement agencies. Representative matters include money laundering and terrorist financing, cybersecurity and data breach response, securities and accounting fraud, insider trading, bribery (including the US FCPA and the UK Bribery Act), and other white-collar criminal and civil matters.

Joseph served as a trial attorney in the DOJ National Security Division's Counterterrorism Section, was appointed a Special Assistant US Attorney for the Eastern District of Virginia, and served on the FBI's 9/11 Review Commission staff. He has testified before Congress on matters relating to international money laundering and terrorist financing. A decorated combat veteran, Joseph is a lieutenant colonel in the US Army Reserve, has served on active duty as a military prosecutor in Europe, the Middle East and Africa, and was awarded the Bronze Star Medal for his service in Iraq.

Joseph earned a law degree from St John's University School of Law, a master of business administration degree from St John's University Peter J Tobin College of Business, and a bachelor of arts degree from Stony Brook University. He is dual-qualified to practise in the United States and as a solicitor in England and Wales, and is also a certified public accountant. In 2019, Joseph was named a Super Lawyer in DC *Super Lawyers* magazine, and a Future Leader in *Who's Who Legal: Investigations*.

Ben Morgan
Freshfields Bruckhaus Deringer

Ben Morgan is a member of Freshfields' global investigations practice in London and a member of the corporate crime group. Ben joined the firm as a partner in 2017. He advises clients on identifying and controlling the risks that arise from regulatory and criminal law enforcement within the domestic and international landscape. Ben practised as a defence lawyer in the City of London before becoming a board member and the joint head of bribery and corruption at the UK Serious Fraud Office (SFO). There, he led some of the SFO's most significant corporate cases and influenced UK policy matters such as the introduction of deferred prosecution agreements, enforcement of the UK Bribery Act and development of the law of corporate criminal liability. He also had a particular focus on building the international relationships necessary to investigate and conclude the most complex matters.

Christopher J Morvillo
Clifford Chance US LLP

Christopher J Morvillo has extensive experience representing corporate and individual clients in criminal investigations and proceedings, internal investigations, and related regulatory and civil matters. With a particular focus on cross-border government and internal investigations, his many representations have involved allegations of accounting fraud, public and foreign corruption, securities fraud, insider trading, economic sanctions violations, trade secret theft, and computer fraud. Mr Morvillo also advises corporations and businesses on related compliance and policy matters.

From 1999 to 2005, Mr Morvillo served as an Assistant US Attorney for the Southern District of New York, where he investigated, tried and handled appeals in a wide variety of criminal cases, including in the area of healthcare fraud, insurance fraud, money laundering, obstruction of justice, counterterrorism and narcotics. In 2005, he received the US Attorney General's Award for Exceptional Service – the Justice Department's highest award for prosecutors – in recognition of his role in the investigation and successful prosecution of a large international terrorism case.

Mr Morvillo was named one of the top five most highly regarded lawyers in the United States for business crime corporate defence in the 2016 edition of *Who's Who Legal*. Mr Morvillo's expertise has also been recognised by numerous other publications, including *Chambers*, *Best Lawyers in America* and *Super Lawyers New York*. Mr Morvillo speaks and writes frequently on government investigations.

David Murphy
Fox Williams LLP

David Murphy is a partner at Fox Williams LLP who specialises in guiding HR directors, boards and in-house legal teams through difficult employment situations, and in advising senior individuals when they join and leave their employers or face problems during their employment.

His corporate client base is focused on the financial services and professional services sectors, and he is experienced in advising on sensitive investigations in both sectors, particularly in respect of allegations relating to breach of duty, discrimination and harassment. His

individual clients include fund managers, investment bankers, directors of listed companies and lawyers. He has advised several individuals at executive committee level on their departures from a major bank. In 2019, he spoke at the Corporate Compliance and Internal Investigations seminar of the Labour Law Commission and Criminal Law Commission of the Union Internationale des Avocats. In the 2019 edition of *The Legal 500*, David was recognised as providing 'consistently pragmatic and timely advice in a calm and reassuring way'.

Stéphane de Navacelle
Navacelle

With more than 15 years' experience in French and US white-collar crime, Stéphanae de Navacelle has participated in several landmark cases involving the US Foreign Corrupt Practices Act and embargo restrictions (OFAC), charges of market abuse and insider trading, fraud (Forex), benchmark manipulation (LIBOR and EURIBOR), investigations by multilateral development banks (World Bank) as well as criminal and internal investigations in Europe, the Americas and Africa. He advises companies with setting up and auditing ethics and compliance programmes; as such he was appointed as independent compliance monitor and expert pursuant to a negotiated resolution agreement by European groups with the World Bank (2018–2019).

A member of the Paris Bar Council (2017–2019), Stéphane de Navacelle is secretary of the International Committee, of the criminal-prospective subcommittee, a member of the ethics committee on professional secrecy (of which he was formerly secretary) and of the ethics committee on conflict of interest; he has also served as ethics investigator.

Stéphane de Navacelle has been identified as a leading practitioner by *Chambers and Partners*, *The Legal 500 France*, *The Legal 500 EMEA*, *Who's Who Legal* and the Expert Guides for white-collar crime and business crime, investigations and stock market litigation.

Stéphane de Navacelle is a regular participant in seminars and is consulted on issues relating to regulatory and criminal investigations in Europe and the United States.

Jillian Naylor
Linklaters LLP

Jillian Naylor is a partner in Linklaters' employment and incentives group in London with particular expertise in contentious and advisory employment matters. She is described as 'extremely knowledgeable' and 'absolutely brilliant and superb' in her area in *The Legal 500* and *Chambers* directories.

Jillian advises her clients on their most sensitive employee relations issues including whistleblowing and discrimination issues, senior and executive level appointments and terminations, and employment aspects of internal and regulatory investigations, as well as performance, conduct and culture issues that arise within a regulatory environment.

Jillian regularly manages employment litigation in the High Court and employment tribunals as well as using methods of alternative dispute resolution such as mediation and conciliation to resolve disputes. She frequently advises clients on the commercial strategies associated with such processes.

Jillian has considerable expertise advising clients on whistleblowing matters. Jillian is a 'thought leader' in the whistleblowing space and has been involved in leading the firm's

'Listen Up' campaign, which aims to focus the whistleblowing discussions on internal behaviours and responses to whistleblowing. As part of this, Jillian produced an e-Learning module with Protect (formerly known as Public Concern at Work). Jillian is also a regular commentator, blogger and speaker on such issues.

Sheila Ng
Rajah & Tann Singapore LLP

Having developed her legal career in both commercial and criminal litigation since joining the firm as a pupil upon graduation in 2007, Sheila Ng has been involved in a broad spectrum of disputes and advisory work. Her practice focuses on commercial and financial disputes and investigations, fraud and asset recovery, as well as corporate insolvency, and she has broad experience and expertise in these areas.

Sheila has advised and represented various international entities in the investigation and prosecution of cross-border claims involving commercial fraud and breaches of fiduciary duties, and the recovery of assets globally. She has also acted for major international banks and brokerages in investigations into regulatory, risk and compliance issues related to matters such as market manipulation, fixing of benchmark rates, layering and spoofing, and insider trading. She has also been at the forefront of major cross-border insolvencies in the region, having acted and continuing to act for the liquidators of Dynamic Oil Trading (part of the OW Bunker Group), MF Global Singapore and various Lehman Brothers Singapore entities.

Sheila was featured as one of 100 female investigations specialists in Global Investigations Review's Women in Investigations 2018, and was also recently recognised in the 2019 Edition of *Who's Who Legal* as a Future Leader in the field of investigations. Sheila is also a Fellow of INSOL International.

Timothy P O'Toole
Miller & Chevalier Chartered

Timothy P O'Toole has been conducting and leading large-scale defence investigations for over 20 years. His practice's main focus is defending enforcement actions and conducting investigations involving the economic sanctions, export controls and anti-money laundering laws. His clients run the gamut, including US and non-US financial institutions and public companies in the aviation, insurance, logistics, manufacturing, and oil and gas sectors. Ranked as one of the nation's leading international trade lawyers by both *Chambers USA* and *The Legal 500*, Mr O'Toole represents companies and individuals at all stages of the process, including defending enforcement actions brought by the US Department of Justice (DOJ), the Treasury Department's Office of Foreign Asset Control (OFAC), the State Department's Directorate of Defense Trade Controls (DDTC) and the Commerce Department's Bureau of Industry and Security (BIS). He also provides companies and individuals with advice on compliance with the US economic sanctions, export controls and anti-money laundering laws, and interacts regularly with the DOJ, OFAC, the DDTC and the BIS in that capacity. Mr O'Toole has substantial experience dealing with criminal and civil regulators and extensive courtroom experience before judges and juries, having appeared in state and federal courts hundreds of times in a variety of civil and criminal proceedings.

Babajide Ogundipe
Sofunde Osakwe Ogundipe & Belgore

Babajide Ogundipe is the senior partner at Sofunde, Osakwe, Ogundipe & Belgore. He has practised as a commercial litigator in Nigeria for 40 years. His asset recovery practice is part of his practice as a commercial litigator, and he has acted on behalf of numerous clients to assist in the recovery of assets lost as a result of fraud and other misfeasance. He has, as a result, gained enormous experience and has come to be recognised as one of Nigeria's leading lawyers in the field.

He was elected a fellow of the Chartered Institute of Arbitrators in 1994 and served as the chairman of the Nigerian branch from 2006 to 2009. He was the first president of the Lagos Court of Arbitration, from February 2010 to February 2014.

He is a frequent speaker in Nigeria and abroad on arbitration, anti-corruption and asset recovery issues and on the regulation of the legal profession. He is the Nigeria representative for FraudNet (which operates under the auspices of the International Chamber of Commerce) and has served as an officer of the executive of the International Bar Association's anti-corruption and regulation of lawyers' compliance committees.

Olatunde Ogundipe
Sofunde Osakwe Ogundipe & Belgore

Olatunde Ogundipe is an investigator/analyst with Sofunde, Osakwe, Ogundipe & Belgore. He studied law at Essex University and electrical and electronic engineering at Loughborough University. Prior to joining the firm in 2018, he had been conducting investigations on a contractual basis for three years.

Danny Ong
Rajah & Tann Singapore LLP

Danny Ong specialises in complex international investigations and commercial disputes across a multitude of industries. In particular, on the banking and finance front, he has led cross-border investigations involving complex financial products, cryptocurrencies, securitisation transactions, commodities, bonds, market manipulation, insider trading, layering and spoofing, interest rate fixing, currency fixing and money laundering, to name a few. In his role as counsel to liquidators, he has also been called upon to oversee cross-border investigations into the affairs of Lehman Brothers, MF Global Singapore, Dynamic Oil Trading (of the OW Bunker Group) and BSI Bank. Danny also has a very broad experience and is well known for his work in cross-border fraud and asset recovery investigations and litigation. He has been recognised in these areas of expertise by international legal directories, with clients describing him as 'a formidable force', 'an excellent litigator', 'our go-to guy', an 'outstanding lawyer', 'very switched on', 'good when you need someone to fight your corner', 'very commercial, he knows when he has to be aggressive and commercially aware at the same time', and with *Who's Who Legal* ranking him as one of 40 Thought Leaders globally in asset recovery.

Tamara Oppenheimer
Fountain Court Chambers

Tamara Oppenheimer has been practising as a barrister at Fountain Court Chambers since 2002, having previously trained and worked as a solicitor in the litigation department at Allen & Overy. She has a broad commercial litigation practice spanning financial services, regulatory, general commercial disputes, professional negligence, insurance and aviation. She is a contributor to *The Law of Privilege*, edited by Bankim Thanki QC. Tamara is regularly instructed on matters concerning privilege and confidentiality, particularly in the regulatory and investigatory context. She appeared as junior counsel for Eurasian Natural Resources Corporation in two recent privilege decisions, *Dechert v. Eurasian Natural Resources Corporation* [2016] 1 WLR 5027 and *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2017] 1 WLR 4205 (at first instance) and [2019] 1 WLR 791 (CA). She is also acting for the CAA in the forthcoming privilege appeals in *R (on the application of Jet 2.com) v. Civil Aviation Authority* [2018] EWHC 3364 (Admin) and *R (on the application of Jet2.com) v. Civil Aviation Authority* [2019] EWHC 336 (Admin).

Meghan Gilligan Palermo
Ropes & Gray LLP

Meghan Gilligan Palermo is an associate at Ropes & Gray in New York, who frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Sherbir Panag
Law Firm of Panag and Babu

Sherbir Panag is one of India's foremost white-collar crime lawyers and a partner at the Law Offices of Panag and Babu. Sherbir's multidisciplinary white-collar crime practice has been listed and ranked by *Chambers and Partners*, *Who's Who Legal* and *The Legal 500*. He was recently recognised as a 'Thought Leader for Business Crime Defence (Corporates)' by *Who's Who Legal* and *Global Investigations Review* and has been ranked as one of the '40 under 40 Rising Stars of India' by *Legal Era*.

Sherbir has led investigations and acted as defence counsel in some of India's highest-profile cases, which have also had an interplay with law enforcement in the United States, Europe and Asia. These matters have involved allegations of bribery and other misconduct under Indian and foreign anti-corruption laws; financial and regulatory fraud; procurement fraud; violation of sanctions laws; and violation of corporate governance norms. Sherbir's representative experience spans the entire spectrum of courts in India, including the Supreme Court of India.

Sherbir is a senior fellow at the Wharton School's Carol and Lawrence Zicklin Center for Business Ethics Research and a member of Cornell University's – Meridian 180. He also serves on the advisory group of the Deutsche Gesellschaft für Internationale Zusammenarbeit's Alliance For Integrity.

Jessica Parker
Corker Binning

Jessica Parker is a specialist criminal and regulatory litigator with expertise in all areas of business and general crime. Jessica has experience defending against all of the major prosecuting agencies and has represented senior figures in several significant SFO investigations, including Rolls-Royce, Barclays and G4S. Jessica has substantial experience in regulatory matters and frequently advises clients within the financial services industry. She frequently acts in international investigations, including international requests for evidence and asset freezing. In her general crime practice, Jessica has represented a number of high-profile individuals in relation to the most serious criminal charges, from serious assault to drugs offences.

Avni P Patel
Walden Macht & Haran LLP

Avni Patel is an experienced litigator and trial attorney who has represented individuals and corporate clients in complex, sensitive and high-profile cases including in federal, state, and local criminal and regulatory matters. Her practice focuses on white-collar criminal defence, government investigations and regulatory enforcement, and complex litigation. At Walden Macht & Haran, Avni was part of the trial team who successfully defended a corporate client in a high-profile public corruption case in the Southern District of New York. They won the only acquittal in the highly contested and publicised four-defendant trial. She also is part of the WMH team representing one of the most significant whistleblowers in sports history. Additionally, Avni was also on the leadership team of the independent monitor named by the US Department of Justice to oversee General Motors' compliance with its obligations under the deferred prosecution agreement (DPA) stemming from its recall of defective ignition switches. Before joining Walden Macht & Haran, Avni served as an Assistant District Attorney for five years in the Bronx County District Attorney's Office. In those five years, Avni tried over 15 felony and misdemeanour cases to verdict – five of them to jury verdict – on charges ranging from attempted murder to grand larceny. Avni is a graduate of Boston University School of Law and Northwestern University.

Angela Pearsall
Clifford Chance

Angela Pearsall is a partner with more than 20 years' experience in the litigation and dispute resolution practice based in Sydney. Recognised in *The Legal 500* as a 'superb, motivated and hardworking' commercial litigator with financial services as a sector strength, Angela has worked on some of the largest and most high-profile matters in the country. Her areas of specialisation are large-scale commercial litigation, class actions, contentious regulatory disputes and investigations. She regularly represents banks and large corporates in regulatory disputes and investigations. She is recognised as a leading lawyer in the 2016 *Doyle's Guide* and the most recent rankings by *Best Lawyers*.

Angela has significant experience in contentious regulatory matters and has assisted clients with internal investigations and reporting. Her strong client base has included global banks and financial services companies, including HSBC, ANZ, CBA, RBS and BNP Paribas.

Angela has worked on a number of high-profile inquiries, including, most recently, under the Charitable Fundraising Act in relation to various Returned Services League entities and the Banking Royal Commission. She has conducted a number of complex fraud investigations and related litigation.

Nichola Peters
Addleshaw Goddard LLP

Nichola Peters is a partner and heads up Addleshaw Goddard's global investigations and contentious regulatory group. She specialises in advising corporates, directors and senior management on regulatory inquiries, financial and corporate crime issues. Key areas involve advising on and carrying out investigations relating to corporate collapse, corruption, sanctions, money laundering, terrorist financing, extradition, information security and fraud issues. As Nichola regularly investigates compliance failings, she is able to provide specialist non-contentious advice on what to look out for, how matters can go wrong and how to minimise that risk. In relation to contentious matters, because Nichola works regularly with clients to conduct due diligence and implement effective compliance programmes, she has an excellent understanding of industry standard practice and what procedures should have reasonably been put in place to prevent compliance failings. Nichola is ranked as a Thought Leader in *Who's Who Legal: Investigations* and *Who's Who Legal: Business Crime Defence*. Nichola was selected by *Global Investigations Review* in 2018 as one of 100 remarkable women investigation specialists operating across the world. Nichola was also named as one *The Lawyer*'s 'Hot 100' lawyers in 2017.

Hayley Pizzey
Latham & Watkins

Hayley Pizzey is an associate in the London office of Latham & Watkins.

Ms Pizzey's broad practice focuses on multi-jurisdictional litigation and regulatory matters. She advises clients on a wide range of disputes with a particular focus on commercial litigation and contentious data protection as well as regulatory investigations.

Ms Pizzey's experience includes claims in the High Court, the Court of Appeal, and the Competition Appeal Tribunal. She has also acted on matters involving the Competition and Markets Authority, the European Commission, and numerous data protection authorities and financial services regulators across the world.

Glenn Pomerantz
BDO USA, LLP

Glenn Pomerantz leads BDO USA LLP's global forensics practice with nearly 35 years of forensic accounting, auditing and consulting experience. Working with multinational organisations and their counsel, Glenn leads cross-border matters that mitigate the risks associated with fraud and corruption. He works with BDO leaders around the globe to respond to clients' needs involving anti-corruption and fraud investigations, forensic technology, compliance and due diligence matters in mature and emerging markets.

Glenn has significant experience in managing engagements involving alleged violations of the Foreign Corrupt Practices Act and UK Bribery Act, and embezzlement, theft and financial reporting fraud. In addition, he has spent much of his career providing expert witness testimony on economic damages, as well as providing litigation and dispute advisory services, including evaluating claims under fidelity bonds and employee dishonesty insurance coverage. He has also served as a court-appointed umpire and referee and as a neutral arbitrator.

Polly Pope
Russell McVeagh

Polly Pope is one of New Zealand's leading financial, construction and insolvency litigators. She was named as Best Lawyer – Litigation in 2016, 2017 and 2018. She has significant expertise in investigations, originating in the years that she spent in practice at Clifford Chance in London, where she acted on several cross-border internal and regulatory investigations. At the time of writing, Polly was a finalist for NZ Lawyer of the Year (Benchmark Litigation Asia Pacific) and had recently been awarded the prestigious Sir Ronald Davison Award by the Arbitrators' and Mediators' Institute (AMINZ). Polly is a fellow of AMINZ and a member of the Council of the New Zealand Legal Research Foundation.

Charlie Potter
Brunswick Group LLP

Charlie Potter advises a broad range of media, telecoms and professional services clients on many communications issues, particularly in the context of legal proceedings, regulatory disputes, mergers and corporate crises. He co-leads Brunswick's litigation, disputes and investigations practice in London. He is also a partner in Brunswick's family business, crisis and cybersecurity practices. Charlie joined Brunswick in June 2012 from his practice as a barrister at Blackstone Chambers, where he specialised in public/administrative and commercial law, in particular broadcasting and media regulation. During his legal practice, Charlie was regularly instructed by statutory regulators in various proceedings, and advised commercial clients on a range of sensitive regulatory issues. Before the Bar, Charlie spent four years at the BBC, including as a producer at the flagship television news and current affairs programme Newsnight.

Elly Proudlock
Linklaters LLP

Elly Proudlock acts in investigations by the Serious Fraud Office (SFO) and other authorities, representing companies and individuals facing allegations of fraud, bribery and corruption, money laundering and other types of misconduct. Key work highlights for Linklaters include working on an SFO investigation for a multinational energy services company, representing a non-UK listed company in a self-report and acting for a UK listed company in an SFO fraud investigation. Previous experience includes representing senior individuals in SFO investigations involving high profile names such as Barclays, ENRC and Rolls-Royce. Elly also regularly advises companies on the whole range of issues relating to business crime, including anti-bribery and corruption and anti-money laundering. Elly is ranked as 'up and coming' in the *Chambers and Partners* directories for Financial Crime: Corporates.

Nicholas Purnell QC
Cloth Fair Chambers

Nicholas Purnell's practice in commercial and business crime and in regulatory and professional disciplinary matters has spanned over four decades. Typically instructed at the early stages of investigations pre-charge, he advises clients in cases under examination by global regulatory and prosecuting authorities including the Serious Fraud Office (SFO), the Financial Conduct Authority, the US Department of Justice and the Securities and Exchange Commission.

The development of collaborative investigations across jurisdictions has brought about the need for teams to be in place to provide joint advice on the impact of managing the response to investigations on a global basis. Nicholas has specialist experience in the development of the appropriate strategy to enable businesses to develop and cope with the resource demands imposed by such investigations.

Nicholas acted for ICBC Standard Bank throughout the first ever deferred prosecution agreement to be approved in the United Kingdom. Following months of negotiations with the SFO, Nicholas appeared before the President of the Queen's Bench Division at the High Court where the terms of the agreement were finalised. This case marked Nicholas's hat-trick of firsts: the first civil settlement with the SFO for Balfour Beatty; the first attempt at a simultaneous global settlement in the United States and the UK with the SFO in *Innospec*; and the combination of this first charge under section 7 of the Bribery Act in achieving this deferred prosecution agreement with the SFO.

Nicholas successfully represented clients in the United Kingdom over allegations made by the SFO against Tesco and Barclays and advised one of the three DePuy International executives who was on trial in Athens.

Amanda Raad
Ropes & Gray LLP

Amanda N Raad, a US lawyer who is also admitted as a solicitor in England and Wales, serves as co-chair of Ropes & Gray's award-winning global anti-corruption and international risk practice. Amanda has substantial experience negotiating with US regulators on behalf of companies and individuals concerning cross-border matters involving corruption, money laundering and other forms of financial fraud. These matters are often subject to scrutiny by foreign regulators, given their multi-jurisdictional nature.

In addition, Amanda proactively works with clients across industries and geographies to identify and mitigate risk. Finally, Amanda advises clients on corporate social responsibility, supply chain compliance and responsible sourcing. Amanda regularly publishes on cross-border issues and is a frequent speaker at conferences, including on sexual misconduct and investigations. Amanda is listed in Global Investigations Review's *Women in Investigations* 2018, *Chambers UK, The Legal 500 UK* and *New York Super Lawyers*.

Samuel Rabinowitz
Fountain Court Chambers

Sam Rabinowitz is a barrister practising from Fountain Court Chambers and specialising in commercial law. He is regularly instructed on matters in which privilege issues arise, and as a pupil assisted counsel for ENRC in the trial of *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2017] 1 WLR 4205. Sam worked as a judicial assistant in the Commercial Court for six months in 2018.

Alberto Rebaza
Rebaza, Alcázar & De Las Casas

Alberto Rebaza is the founding and managing partner of Rebaza, Alcazar & De Las Casas. As partner, he co-leads the mergers and acquisitions and corporate areas. In addition to his master's degree from the University of Virginia, he has studied at Georgetown University and in England.

Alberto has been consistently considered by legal rankings as a leading lawyer in mergers and acquisitions. He has been a speaker at conferences in Dublin, São Paulo, Bogotá, Panama City, Barcelona, New York City, Mexico City and Singapore, among others.

He has been a director for several companies and organisations, such as Edegel (energy), Rigel Peru (insurance), Liderman (services), Amrop (services), IPAE, Pesquera Alexandra (fishing) and YPO.

Very much involved in the arts world, Alberto is vice president of the Museum of Art of Lima, a member of the international patronage committee of the Reina de Sofia Museum and a member of the Latin American Circle at the Guggenheim Museum in New York.

Conor Reardon
Jones Day

Conor Reardon is an associate at Jones Day in New York City. After graduating from the Duke University School of Law in 2014, he served as a law clerk to Judge Robert N Chatigny, of the US District Court for the District of Connecticut, Judge José A Cabranes, of the US Court of Appeals for the Second Circuit, and Chief Justice John G Roberts Jr, of the US Supreme Court. At Jones Day, he focuses on appellate advocacy and critical motions practice, with a particular emphasis on white-collar criminal defence.

Marcus Reischl
Gleiss Lutz

Dr Marcus Reischl is an associated partner and a member of the compliance and investigation practice at Gleiss Lutz. Marcus advises domestic and international clients on compliance, and represents firms in court and arbitration proceedings. He specialises in strategic compliance advice as well as setting up, implementing and developing compliance structures. Marcus regularly assists companies with internal investigations for detecting irregularities, advising on their impact, in particular with regard to judicial and extrajudicial disputes with business partners and co-operation with the authorities.

Marcus studied at the universities of Freiburg (Breisgau), Munich and Passau. He has been with Gleiss Lutz since 2013. In 2012. Marcus worked for an international law firm in Toronto, Canada. He is a member of the Institution of Arbitration e.V. (DIS) and the German Lawyers' Association (DAV). Marcus speaks German and English.

Karen Reynolds
Matheson

Karen Reynolds is a partner in the commercial litigation and dispute resolution department at Matheson and co-head of the firm's regulatory and investigations group.

Karen has a broad financial services and commercial dispute resolution practice. She has more than 10 years' experience in providing strategic advice and dispute resolution to financial institutions, financial services providers, domestic and internationally focused companies and regulated entities and persons. She advises clients in relation to contentious regulatory matters, investigations, inquiries, compliance and governance-related matters, white-collar crime and corporate offences, commercial and financial services disputes, anti-corruption and bribery legislation, and document disclosure issues.

Karen has substantial experience in corporate restructuring and insolvency law matters, having had a lead role in some of the most high-profile corporate rescue transactions of the last 10 years. She advises liquidators, regulators, directors and insolvency practitioners in relation to corporate offences and investigations, shareholder rights and remedies, directors' duties, including in relation to fraudulent and reckless trading, and disqualification and restriction proceedings.

Charles D Riely
Jenner & Block LLP

Charles Riely is a partner at Jenner & Block and a member of its investigations, compliance and defence, markets and trading and securities litigation and enforcement practices. Before joining Jenner & Block, he served as a lawyer at the SEC for more than a decade, most recently as assistant regional director for the SEC's Division of Enforcement. While with the SEC, he worked on matters involving disclosure failures by public companies, alleged fraud and regulatory violations by investment advisers and broker-dealers, insider trading, anti-money laundering violations, 'spoofing' and other forms of market manipulation, failure-to-supervise violations, the adequacy of firms' cybersecurity procedures and protections, and a variety of other fraud and regulatory matters. Mr Riely also coordinated investigations with the US Department of Justice and worked on more than a dozen publicly filed SEC enforcement actions in which criminal authorities filed a parallel case. He graduated from the University of Michigan Law School and served as a law clerk to the Honorable Frank Maas of the US District Court for the Southern District of New York. He is admitted to practise in New York.

Elizabeth Robertson
Skadden, Arps, Slate, Meagher & Flom (UK) LLP

Elizabeth Robertson is a partner in Skadden's government enforcement and white-collar crime group in London.

She advises on multi-jurisdictional business crime and regulatory matters around the world. Ms Robertson has played a role in many of the most important criminal and regulatory investigations in the United Kingdom over the past 20 years, giving her significant understanding of the priorities of the UK prosecuting authorities such as the SFO, the FCA, HMRC, and the Competition and Markets Authority. She has particular experience in corruption, money laundering, economic sanctions and criminal tax cases. Ms Robertson has also advised on criminal cartel matters, and regularly assists with governance and compliance issues as well as proceedings brought by professional and regulatory bodies. She has successfully defended clients on enforcement actions brought by multiple agencies and responded to coordinated dawn raids in the UK and overseas. Ms Robertson also has experience in ancillary matters such as extradition and mutual legal assistance and applying to Interpol for access to information or for information to be amended or deleted.

She is also an accomplished speaker on international business crime.

Flavio Romerio
Homburger

Flavio Romerio is the managing partner of Homburger and heads the white collar and investigations team of the firm. He has extensive experience with the challenges facing Swiss clients appearing before United States courts and regulators.

Flavio Romerio represents clients in investigations by Swiss and foreign government agencies, has led large-scale internal investigations of Swiss clients, and has represented them before Swiss and US regulators, including the US Department of Justice and the Office of Foreign Assets Control. Flavio Romerio regularly advises corporations and their directors and managers on all aspects of white-collar crimes.

Emmeline Rushbrook
Russell McVeagh

Emmeline Rushbrook specialises in commercial and financial dispute resolution, regulatory compliance and enforcement, and public and administrative law. She has extensive experience in advising on regulatory investigations, internal investigations and public inquiries, and regularly advises clients on compliance with New Zealand consumer and financial services laws and on related law reform issues. Emmeline brings a global perspective to her practice, having spent nine years working at Clifford Chance in London. She rejoined Russell McVeagh in 2014 and continues to act frequently on matters that have an international dimension.

Ali Sallaway
Freshfields Bruckhaus Deringer

Ali Sallaway is co-head of Freshfields' global investigations practice in London and a member of the corporate crime group, and she has been a partner at the firm since 2005. With a record of acting on significant cross-border and domestic investigations for clients in all sectors, Ali specialises in particular on corporate and financial crime defence and regulatory enforcement actions. She has significant expertise handling fraud, false accounting, bribery and corruption, money laundering and terrorism matters as well as acting in relation to market abuse, disclosure and listing obligations for listed companies. Highlighted as one of the The Lawyer's Hot 100 for 2015, Ali is recognised as a leading individual in corporate crime, contentious financial services and investigations by all the major directories.

Richard Sallybanks
BCL Solicitors LLP

Richard Sallybanks has been a partner at BCL since 1999 and specialises in complex business crime and regulatory defence work.

Richard has been involved in numerous SFO, FCA, HMRC and CMA investigations and prosecutions, together with associated restraint and confiscation proceedings. His recent SFO experience includes the Alstom, Barclays Qatar and Tesco investigations (acting for senior individuals under suspicion), as well as acting for Robert Tchenguiz in the SFO's Kaupthing Bank investigation (including the successful judicial review challenge to SFO search warrants). Richard has acted in a number of FCA criminal and regulatory investigations for brokers, traders and senior executives, including in relation to allegations of insider dealing and market abuse. He is experienced in cartel investigations, both domestic investigations conducted by the CMA and cross-border antitrust investigations (including those conducted by the US DOJ). Richard is also experienced in the international mutual legal assistance regime, and in leading and co-ordinating teams of lawyers in multi-jurisdictional investigations.

Sandrine dos Santos
Navacelle

Before joining Navacelle, Sandrine dos Santos worked in an elite French litigation boutique and at the Paris Prosecutor's Office from 2007 to 2010. She dealt with cases relating to economic and financial crime or organised crime and damage to persons or property, and acquired a strong expertise in white-collar crime.

Ms dos Santos has worked on complex international corruption matters involving high-profile political stakeholders and large-scale companies in Africa and South America. She also handled sensitive LIBOR-related matters.

Ms dos Santos has assisted clients in setting up global compliance training. She is a regular participant at conferences organised by the French Institute for Higher National Defence Studies.

David Sarratt
Debevoise & Plimpton LLP

David Sarratt is a partner in Debevoise's litigation department. He is a seasoned trial lawyer whose practice focuses on government enforcement actions, internal investigations and complex civil litigation for financial institutions and other clients. Mr Sarratt has particular experience in matters relating to compliance with the Bank Secrecy Act and the Foreign Corrupt Practices Act, as well as with novel enforcement issues arising from new technologies. Prior to joining the firm, Mr Sarratt served as an assistant United States attorney in the Eastern District of New York. As a federal prosecutor, Mr Sarratt supervised and participated in a wide variety of investigations and prosecutions, involving international terrorism, cybercrime, financial and healthcare fraud, racketeering and other crimes. He successfully tried numerous cases to verdict and briefed and argued appeals in the US Court of Appeals for the Second Circuit.

María Lorena Schiariti
Marval O'Farrell & Mairal

María Lorena Schiariti is a partner in the regulatory and administrative law team and the compliance, anti-corruption and investigations team.

In view of the wide variety of international clients subject to the US Foreign Corrupt Practices Act or the UK Bribery Act, she has focused on advising on issues relating to public ethics, anti-corruption, transparency policies and investigations.

Ms Schiariti holds a law degree with a specialisation in administrative law from the University of Buenos Aires, Argentina (1997) and attended the master's in law and economics course at the Torcuato Di Tella University, Argentina (2001–2002). She is currently a professor on the postgraduate course in compliance organised by the Austral University and the Business Institute of Argentina.

She received the Client Choice Award, Public Law (International Law Office, 2018) and she has been listed by *Chambers and Partners Latin America* as a Leading Individual (2009–2019), as a Leading Lawyer by *The Legal 500* (2012–2019) and as Approved Administrative Law Private Practitioner by *LACCA* (2014–2019). She was also included in the list of corporate lawyers to know and compliance lawyers to know by *Latin Lawyer* (2014), *100 Women in Investigation* by *Global Investigation Review* (2015) and as one of the 40 best Argentine lawyers under 40 by *Latin Lawyer* (2003).

Kirsten Scott
Clifford Chance

Kirsten Scott is a counsel in the litigation and dispute resolution practice based in Perth. She specialises in regulatory matters, including white-collar crime, investigations and enforcement, and directors' duties. Prior to joining Clifford Chance, Kirsten worked for the Commonwealth Director of Public Prosecutions Office for more than 10 years in a variety of Australian jurisdictions specialising in commercial and taxation crime. Her work included acting as a senior assistant director for the Commercial Prosecutions branch in Western Australia. This experience gives Kirsten a unique insight into the operation of government agencies and regulatory frameworks.

Kirsten sits on the Law Society of Western Australia's Criminal Law committee and the Competition and Consumer Committee of the Law Council of Australia.

Most recently, Kirsten has advised corporations, individuals and boards on regulatory investigations such as insider trading, misleading and deceptive conduct, continuous disclosure, anti-corruption and market manipulation, including providing advice on corporate governance issues.

Kirsten is regularly retained by individuals, boards and corporate entities in relation to criminal allegations of insider trading and has been involved as an adviser in some capacity in the majority of market-related, contested white-collar criminal matters before Australian courts in recent years.

Kirsten is also the secretary for the Australian Chapter of the Women's White Collar Defense Association.

Judith Seddon
Ropes & Gray LLP

Judith Seddon specialises in white-collar crime, fraud, corruption, and regulatory and criminal investigations and prosecutions. She has deep experience and expertise in advising corporates, financial institutions and individuals in complex investigations and prosecutions, domestically and cross-border, as suspects and as witnesses. She has worked, and is working, on some of the most complex and high-profile investigations and prosecutions. Judith is consistently ranked as a band 1 leading practitioner by *The Legal 500* and *Chambers*. *Who's Who Legal* 2018 named Judith Business Crime Lawyer of the Year and lists her on a shortlist of 10 Thought Leaders. *Who's Who Legal* describes her as 'one of the most highly regarded investigations lawyers in the United Kingdom, highlighted for her "brilliant" work on behalf of both corporates and individuals'.

Sean Seelinger
Ropes & Gray LLP

Sean Seelinger, counsel at Ropes & Gray in London, frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Pedro Serrano Espelta
Marval O'Farrell & Mairal

Pedro Serrano Espelta is a partner at Marval, O'Farrell & Mairal and has been a member of the firm since 1997. He is the head of Marval's compliance, anti-corruption and investigations practice and has led numerous local and international investigations in the field, including asset tracing and recovery cases. He also has extensive experience in corporate law, mergers and acquisitions, and oil and gas.

As the Argentine representative to the International Organization for Standardization in 2016, he participated in the preparation of the Anti-Bribery Management standard 37001.

Pedro received his law degree from the National University of the Littoral in 1992. He was a visiting scholar at the University of California at Berkeley from 1993 to 1995 and received a master of laws degree (LLM) from the University of California, Los Angeles, in 1997.

He was foreign associate at the law firm The Americas Law Group in San Francisco, California, from 1993 to 1996, where he worked on complex international agreements.

Pedro is a frequent writer in specialist publications and a regular speaker at international conferences and seminars on issues relating to his expertise.

He is a member of the Buenos Aires Bar Association and is ranked by *Chambers Latin America* as a top practitioner in the field.

Gabriel Sidere
CMS Cameron McKenna Nabarro Olswang LLP SCP

Gabriel Sidere is the managing partner of the CMS office in Bucharest and head of the dispute resolution and white-collar crime practice in Romania.

Gabriel advises on complex criminal disputes, particularly those relating to fighting corruption and fraud. He also regularly advises on forensic investigations concerning criminal law and regulatory matters. His recent cases include securities regulatory inquiries (market manipulation, insider trading, etc.), and investigations by Romania's anti-corruption agency (DNA) and the organised crime and terrorism investigation agency (DIICOT). For many years, Gabriel has assisted publicly listed companies to conduct internal investigations into allegations of wrongdoing. These investigations have been in a wide variety of industries, including energy, financial services, healthcare and infrastructure.

Gabriel's litigation practice includes the representation of clients in complex business litigation and international arbitrations matters. These representations include strategic advice on investment-related disputes, helping clients manage responses to government inquiries and representing clients in high-level negotiations. Gabriel has successfully argued motions on bilateral investment treaty claims before the International Centre for Settlement of Investment Disputes, a member of the World Bank Group.

Gabriel is an accredited mediator and certified advanced negotiator with the Centre for Effective Dispute Resolution, and has been a member of the Bucharest Bar Association since 1997.

Diego Sierra
Von Wobeser y Sierra, SC

Diego Sierra is head partner of the bankruptcy and restructuring and anti-corruption and compliance practices of Von Wobeser y Sierra. He has more than 15 years of experience and frequently acts as counsel in complex commercial litigation and commercial arbitration disputes. Diego represents several national and international clients in the resolution and prevention of commercial disputes. He has advised global Fortune 500 companies and financial institutions in the United States and Mexico in investigations under the US Foreign Corrupt Practices Act and due diligence matters.

Grace C Signorelli-Cassady
Jenner & Block LLP

Grace Signorelli-Cassady is an associate at Jenner & Block focusing on investigations, compliance and defence. Her experience includes assisting corporates in responding to government enquiries, including by US and European enforcement authorities, assisting corporates in conducting complex, worldwide internal investigations, including in connection with allegations of money laundering, bribery and corruption, and representing individuals in white-collar matters, including for misrepresentations to investors and mail and wire fraud. She has also drafted six *amicus curiae* briefs regarding white-collar and criminal law issues, five of which were filed with the US Supreme Court. Prior to joining Jenner & Block, Ms Signorelli-Cassady served as a law clerk to the Hon. Roslyn O Silver of the US District Court for the District of Arizona, during which time she assisted with matters taken by designation in the US Court of Appeals for the Ninth Circuit. Ms Signorelli-Cassady received her law degree from Harvard Law School, where she was the managing editor of the *Harvard Journal on Legislation*, selected as a criminal justice fellow and trained in negotiation techniques, eventually helping to teach negotiation strategy to executives from around the world in connection with the Harvard Negotiation Institute. She is admitted to practise in Illinois.

Daniel Silver
Clifford Chance US LLP

Daniel Silver is a partner at Clifford Chance US LLP, where he focuses on regulatory enforcement and white-collar criminal defence. Dan represents both individuals and corporations in matters before the Department of Justice and other federal and state enforcement agencies, and counsels clients on risk mitigation strategies with respect to cybersecurity, anti-corruption, sanctions and anti-money laundering issues. Prior to joining Clifford Chance, Dan spent 10 years as a federal prosecutor, serving in several senior leadership positions and overseeing the national security and cybercrime unit within the United States Attorney's Office for the Eastern District of New York. Dan received his undergraduate degree from Brown University and his JD, *magna cum laude*, from NYU School of Law.

Christoph Skoupil
Gleiss Lutz

Dr Christoph Skoupil is an associated partner and a member of the compliance and investigation practice at Gleiss Lutz. Christoph advises companies on all aspects of white-collar crime and compliance. He specialises in defending companies and advising them in cases of criminal offences against the corporation. This includes both internal investigations and preventive measures.

Christoph studied at the University of Mainz. He joined Gleiss Lutz in 2015. From 2013 to 2015, Christoph worked at a leading boutique law firm specialising in white-collar crime. From 2010 to 2012, he lectured in criminal law at the University of Mainz. Christoph speaks German and English.

Nicole Sliger
BDO USA, LLP

Nicole Sliger is a partner in the New York office of BDO USA, LLP with nearly 20 years' experience providing accounting services to private and publicly traded businesses. She assists organisations and their counsel with matters involving alleged financial statement irregularities, management fraud and compliance issues, as well as investigating fraud perpetrated by rogue employees. She also provides monitoring and oversight services to companies required to comply with settlement terms and corporate compliance programmes.

Nicole was the primary project leader for the National Mortgage Settlement engagement, assisting the monitor in evaluating large financial institutions' compliance with the new mortgage servicing rules and other settlement terms. She has been involved in a number of securities litigation matters, monitorships, white-collar crime, investigations and financial statement fraud cases, helping counsel evaluate and interpret auditing, accounting, financial reporting and compliance issues.

Nicole has managed significant corporate investigations for Fortune 500 companies across various industries. She assists counsel in identifying relevant documents during discovery and preparing for depositions of witnesses concerning testimony that involves the application of GAAP and GAAS. She supervises large-scale electronic document reviews and drafts reports used in filings with the US Securities and Exchange Commission and other regulators. She has also led a number of internal and shadow investigations and matters involving whistleblower allegations.

Andrew Smith
Corker Binning

Andrew Smith specialises in business crime, including SFO, NCA and police investigations relating to fraud, bribery/corruption and money laundering, as well as regulatory inquiries brought by the FCA into market abuse and market misconduct. Andrew also regularly acts for individuals facing extradition to a range of countries and provides related advice on Interpol and criminal mutual legal assistance. Case highlights include: acting for individuals in SFO investigations, including Tesco, BAT, Petrofac, Unaoil, LIBOR and EURIBOR; representing a defendant in the FCA's largest prosecution of insider dealing (Operation Tabernula) and FCA regulatory investigations concerning LIBOR and FX; advising businesses on alleged breaches of export controls and trade and financial sanctions; acting for executive counsel to the Financial Reporting Council on disciplinary investigations into major firms of accountants; and representing Shrien Dewani in the South African request for his extradition for the offence of murder.

Meghan K Spillane
Goodwin

Meghan Spillane, a partner in Goodwin's securities litigation and white-collar defence group, focuses her practice on white-collar criminal defence, corporate internal investigations, and complex business and financial litigation. Her experience includes federal criminal and civil investigations, securities class actions and derivative suits, SEC actions, and complex civil litigation matters. In addition to her other client work, Ms Spillane represents indigent criminal

defendants on a *pro bono* basis in a variety of state and federal matters. Ms Spillane is a member of the bar of the State of New York and is admitted to practise before the US District Court for the Southern District of New York. Ms Spillane was named as a 2018 Law360 Rising Star in 'White Collar', was recognised in Who's Who Legal's *Investigations 2019 – Future Leaders* and has been named consistently by *New York Super Lawyers* as a leading white-collar defence practitioner from 2015 to 2019.

Christian Steinle
Gleiss Lutz

Dr Christian Steinle is a partner and co-head of the compliance and investigation practice of Gleiss Lutz. Christian has considerable experience in European and international antitrust law and compliance investigations. He focuses on cartel cases and private antitrust litigation, merger control, online and distribution antitrust law, antitrust compliance programmes and internal investigations.

Christian studied in Tübingen, Fribourg (Switzerland), Bonn and Speyer. He has been a partner at Gleiss Lutz since 2008. In 2004, he was seconded as in-house counsel to a multinational group, where he specialised in international antitrust litigation. He is a member of the Association for the Study of Antitrust Law, the International Bar Association (IBA) and the American Bar Association, and belongs to the IBA Merger Working Group. Christian speaks German, English and French.

Tom Stocker
Pinsent Masons LLP

Tom Stocker is a partner. He specialises in advising businesses on corporate criminal law, regulatory enforcement, internal investigations and compliance. Tom is qualified in Scotland and England and Wales and is ranked in Band 1 by *Chambers and Partners* for corporate crime and investigations (Scotland) and by *The Legal 500* for criminal fraud (Scotland). He has a particular specialism in corporate investigations by Police Scotland and the Crown Office and Procurator Fiscal Service, and in the operation of Scotland's corporate self-reporting and civil settlement regime. He also defends companies and individuals in regulatory enforcement cases brought by the likes of the Gambling Commission, Financial Conduct Authority, HM Revenue and Customs, Ofgem, Office of Financial Sanctions Implementation, and Health and Safety Executive.

Chris Stott
Ropes & Gray LLP

Chris Stott is a member of Ropes & Gray's litigation and government enforcement practice group, based in London. Chris focuses his practice on criminal, contentious regulatory and internal investigations.

Chris has more than 10 years' experience in advising and representing individuals and corporations in connection with investigations and prosecutions by criminal and regulatory enforcement authorities in the United Kingdom and numerous other jurisdictions.

Chris also assists clients with designing and implementing effective compliance and governance arrangements to anticipate and respond to regulatory change.

Chris was previously seconded to a multinational bank to advise the bank and senior executives on its Senior Managers and Certification Regime implementation programme.

Chris joined Ropes & Gray in 2018 from a magic circle firm in London.

Richard M Strassberg
Goodwin

Rich Strassberg, chair of Goodwin's white-collar crime and government investigations practice and a former member of the firm's executive committee, specialises in white-collar criminal defence, SEC enforcement proceedings, FCPA compliance and investigations, internal investigations, and complex business and financial litigation. Mr Strassberg is a Fellow of the American College of Trial Lawyers, one of the premier legal associations in America. He has twice been recognised by *The American Lawyer* as 'Litigator of the Week' as a result of his securing extraordinary victories in some of the most closely followed white-collar trials in the country. He is also acknowledged by his peers as being one of the finest white-collar attorneys, twice being cited in Law360 by white-collar partners at other firms as being the white-collar lawyer that impressed them, or that they most feared to go up against in court. Mr Strassberg is consistently ranked in Band One by *Chambers USA* as among the top New York-based white-collar defence lawyers, is rated as being among the Top 100 lawyers in New York by *New York Super Lawyers* and is regularly included in *The Best Lawyers in America* and other surveys of the top white-collar litigators in the country. Mr Strassberg co-authors a quarterly column on Federal Civil Enforcement in the *New York Law Journal*, authored a chapter in the book *Beyond A Reasonable Doubt*, has published numerous articles in various legal periodicals, including several on the FCPA, has been a legal commentator on numerous programmes, including NPR, Fox News, Dateline and the Financial Management Network, and has been a guest speaker for various organisations, including the American Bar Association, the New York Council of Defense Attorneys, and the Federal Bar Council. Prior to joining the firm, Mr Strassberg was the Chief of the Major Crimes Unit in the US Attorney's Office for the Southern District of New York, responsible for supervising approximately 25 Assistant US Attorneys in the prosecution of complex white-collar criminal cases.

Eric H Sussman
Reed Smith LLP

Eric Sussman is a partner in Reed Smith's global regulatory enforcement group based in Chicago; his practice focuses on white-collar criminal defence and complex internal investigations. Eric was a deputy chief in the Financial Crimes and Special Prosecutions Unit of the United States Attorney's Office in Chicago for more than nine years and recently served as the first assistant state's attorney for Cook County. In more than two decades of practice, Eric has tried more than 35 federal and state cases, briefed and argued multiple appeals before the US Court of Appeals, and directed hundreds of investigations. Eric has handled numerous complex civil and white-collar criminal matters for corporations and executives in courts throughout the United States. Specifically, he has directed internal investigations involving the Foreign Corrupt Practices Act, the False Claims Act, insider trading issues, Dodd-Frank whistleblower provisions and healthcare fraud allegations.

Lisa Tenorio-Kutzkey
DLA Piper LLP

Lisa Tenorio-Kutzkey (LT-K) focuses exclusively on white-collar matters in all phases of US federal government prosecution and investigation, with a focus on criminal antitrust defence, FCPA and complex internal investigations.

Lisa is a leader of DLA Piper's global cartel practice, a former trial attorney with the US Department of Justice's Antitrust Division and a former Special Assistant US Attorney for the US Attorney's Office for the Northern District of California. Fortune and Global Fortune 100, 200 and 500 companies and their executives routinely turn to Lisa for assistance in price-fixing, bid rigging and market allocation conspiracy matters. For more than a decade, she has successfully prosecuted or defended clients in nearly every major criminal cartel investigation by the Antitrust Division. Lisa has represented companies and individuals in a variety of sectors, including the automotive, aircraft and ocean transportation, telecommunications, semi-conductors, pharmaceuticals, construction, chemicals, industrial products, real estate and technology, and other electronic components industries.

In addition, Lisa has extensive experience in all facets of FCPA investigations, defence and compliance. She has directed and conducted cross-border investigations of FCPA and other anti-corruption and related compliance matters. Her practice is global in scope, with experience in Argentina, Belize, Brazil, Canada, Chile, China, Costa Rica, Ghana, Honduras, Hong Kong, India, Korea, Mexico, the Philippines, Russia, Thailand and Venezuela.

Femi Thomas
Nokia Corporation

Femi Thomas is vice president and global head of ethics and compliance investigations at Nokia. Femi is a US-qualified attorney who prior to joining Nokia in April 2017 worked in the white-collar and regulatory enforcement practice at Crowell & Moring LLP, Washington, DC, and then at Weatherford International in both legal and compliance roles and executive business roles. Femi has a *juris* doctorate degree and holds an executive MBA from the University of Oxford.

Olga Tocewicz
Pinsent Masons LLP

Olga Tocewicz is a senior associate specialising in white-collar crime and corporate defence. Olga has extensive experience in advising both companies and senior individuals subject to investigation or prosecution by the UK's major law enforcement agencies in relation to allegations of financial crime, including fraud, insider trading, bribery and money laundering. Olga also provides advice in relation to the implementation of effective compliance programmes and delivers training on the topic.

Luke Tolaini
Clifford Chance

Luke Tolaini is a partner in Clifford Chance's international investigations practice. He has over 20 years' experience of investigations – many of these matters involving cross-border

enforcement and related litigation. His domestic focus has been on matters involving the UK's Serious Fraud Office, Financial Conduct Authority, and the Competition and Markets Authority – including negotiating one of the five DPAs agreed to date in the United Kingdom – while his international practice has frequently involved engaging with US, European and Asian authorities on matters involving corruption, fraud, cartels, money laundering and market irregularities. He is also a lead partner in Clifford Chance's risk team, advising clients on the management and prevention of business conduct risk and crisis management. He is a member of the editorial board of *Global Investigations Review*.

Anne M Tompkins
Cadwalader, Wickersham & Taft LLP

Anne M Tompkins is a partner in Cadwalader's white-collar defence and investigations group, resident in the Charlotte, North Carolina, and Washington, DC, offices, and a member of the firm's management committee. Her practice focuses on representing companies and financial institutions, as well as their officers and directors in criminal, civil and administrative investigations. Anne has extensive experience in crisis management, internal investigations and enforcement matters across a variety of industries, including financial services, higher education and government contracting.

Anne was the United States Attorney for the Western District of North Carolina from April 2010 to March 2015. She led numerous high-profile, complex criminal and civil investigations during her tenure, including a public corruption case involving the former mayor of Charlotte, the national security case against former general and CIA director David Petraeus, numerous securities and financial fraud cases, and significant matters in the mortgage-backed securities business.

Prior to her recent service as US Attorney, Anne was a partner in the white-collar defence practice of a national law firm. In over 20 years' experience in government and private practice, Anne has tried more than 30 cases to verdict, and successfully represented clients in, among other matters, investigations involving the mortgage practices of a national homebuilder, Medicare reimbursements to a cardiac care hospital, and anti-kickback and reimbursement compliance at a national dialysis services provider.

Filiz Toprak Esin
Gün + Partners

Filiz Toprak Esin is a managing associate at Gün + Partners and has been working for the firm since 2006. Her practice is focused on corporate and mergers and acquisitions (M&A), competition and business crimes and anti-corruption.

Filiz has been involved in various M&A deals and has assisted several clients with investments in Turkey. Filiz is providing services to clients on daily transactions, from establishment to liquidation.

Filiz has broad experience in compliance matters, including competition and white-collar crimes. She has assisted various major multinational clients in their fight against corruption and provides preventive advice about their compliance process. At the same time, she represents executives of clients before relevant authorities and courts regarding white-collar crime-related investigations and court actions.

Alexandros Tsagkalidis
Anagnostopoulos

Alexandros Tsagkalidis is a member of the Athens Bar (2009). He received his education at the School of Law, National University of Athens (2007) and completed his postgraduate studies at the same university in criminal law and criminal procedure (LLM, 2011). He is experienced in fraud, bribery, money laundering and asset recovery cases. Alexandros is a member of the legal experts advisory panel of Fair Trials International.

Nicholas Turner
Clifford Chance

Nicholas Turner is a registered foreign lawyer in Clifford Chance's Hong Kong litigation and dispute resolution team, and specialises in financial crimes, including economic sanctions and anti-money laundering advisory in the financial services sector. He is admitted in the State of New York and is a certified anti-money laundering specialist.

Nicholas' experience in North America and Asia includes anti-money laundering and sanctions consent-order remediation for a major US financial institution, anti-money laundering and sanctions risk assessments for a US financial institution, and sanctions advisory for a major US financial institution in Asia. His practice covers new product approval, know-your-customer and product advisory, analysis of wire transfers, customer accounts, investment banking deals, and other transactions under anti-money laundering and sanctions regulations. He offers counsel on investigations, testing and remediation of know-your-customer, sanctions screening and related internal compliance controls, and analysis and advisory in line with US, UN and national sanctions regulations in North America and Asia, and anti-money laundering and sanctions training.

Serrin A Turner
Latham & Watkins

Serrin Turner is a partner in the New York office of Latham & Watkins, where he is a member of the firm's information law, data privacy and cybersecurity practice, white-collar defence and government investigations practice, and complex commercial litigation practice.

A former federal prosecutor and experienced trial lawyer, Mr Turner represents financial institutions and corporations in complex civil litigation, white-collar criminal defence matters, internal corporate investigations, and crisis-management situations, including data breaches and other cybersecurity incidents.

Prior to joining Latham, Mr Turner served for six years as an Assistant US Attorney for the Southern District of New York, where he was the Office's lead cybercrime prosecutor. In that role, Mr Turner handled a wide range of cybercrime investigations and prosecutions, including matters involving computer hacking, data breaches, black-market websites, trafficking in stolen payment card and personal identity information, and money laundering through digital currencies.

Mr Turner's representative experience includes leading the response to a credit card breach experienced by a national retailer, including overseeing the breach investigation. He has also assisted various companies and financial institutions on responding to data breaches and other cybersecurity incidents, including supervising forensic investigations of the incidents.

Heloísa Barroso Uelze
Trench Rossi Watanabe

Heloísa Barroso Uelze joined the firm in 2000 and became a partner in 2005. She is currently the head of the Brazilian public law, government relations and regulatory, and ethics, compliance and investigations practice group. Mrs Uelze has vast experience of working in compliance matters, representing clients both before public administration and the judiciary department. On numerous occasions she has dealt with the federal and state public prosecutors' offices in negotiating deals in matters that involved Brazil's Improbity Law and Clean Companies Act. She has also defended clients' interests before several courts of accounts (at federal, state and municipal levels). Mrs Uelze also works with clients in strengthening their compliance areas, by improving both the internal rules and the mechanisms to enforce those rules. She prepares and reviews internal policies and guidelines, and also provides speeches and training to clients' teams, to make sure everyone is aware of the applicable rules.

Mrs Uelze is recognised as a leading practitioner in such areas of law by various international publications, such as *Chambers*, *LACCA*, *Análise Advocacia* and *PLC*. She graduated at the Pontifical Catholic University of São Paulo Law School and is a specialist in administrative law, constitutional law, tax law and civil procedure.

Thomas Voppichler
Knoetzl

Thomas Voppichler is a counsel at KNOETZL. His practice is focused on business crime matters, asset recovery and international litigation.

An expert in all areas of white-collar crime, Thomas delivers an effective experience to clients through high-profile criminal proceedings, especially in aggressive pursuit of injured parties' recovery of damages suffered through embezzlement, fraud and bribery.

Thomas has extensive experience in conducting internal and external corporate investigations, essential both for revealing internal misconduct and enhancing compliance, and for gathering evidence and preparing for criminal and civil enforcement claims for injured companies.

Thomas also routinely acts as defence counsel in cases involving corporate and business crimes, and handles mission-critical cases for national and international clients. Thomas also maintains significant, active and current expertise in asset tracing and recovery techniques, applied successfully in a wide array of jurisdictions.

With many years of experience in high-profile, complex litigation, Thomas is frequently active as legal counsel to international corporates. In those disputes, mostly concerning the banking, insurance, construction and corporate sectors, clients gain advantage from Thomas's extensive knowledge and experience in proceedings with interim measures, large amounts at stake, and time-sensitive missions.

Donna Wacker
Clifford Chance

Donna Wacker is the head of the Hong Kong contentious regulatory team. She is admitted in Hong Kong, Australia, and England and Wales and has been practising in Asia since 1999.

Donna advises on contentious and advisory regulatory matters in the financial sector, and in complex banking and commercial litigation. She has advised investment banks and brokerages in a wide range of regulatory investigations, including on insider dealing and other forms of market manipulation, global investigations into rate fixing, short selling, algorithmic trading issues, sponsor work for initial public offerings, reporting failures, and a range of system and control issues. Donna is currently advising on a number of litigation matters involving alleged mis-selling of derivatives and other structured products. Donna also leads the firm's contentious insolvency practice and is advising a number of financial institutions in respect of their resolution planning activities.

Donna is ranked as a leading individual in *Chambers* for litigation, contentious regulatory, and restructuring and insolvency work, and is also recognised in *The Legal 500*.

Rebecca Kahan Waldman
Dechert LLP

Rebecca Kahan Waldman is a partner in Dechert's white-collar and securities litigation group. Ms Waldman focuses her practice on complex commercial and securities disputes with an emphasis on litigation involving the banking and financial services sectors, white-collar and internal investigations, and e-discovery. She also has significant trial experience and has served as trial counsel in a number of federal, state and bankruptcy litigations. Ms Waldman is actively involved in recruiting and is also in charge of the New York Office Women's Initiative.

Her significant representations include advising the former chief executive officer of a registered futures commission merchant and broker dealer in civil litigations and congressional and regulatory inquiries arising out of the bankruptcy of a former employer; the former chief risk officer of Fannie Mae against securities fraud charges filed by the SEC in the Southern District of New York; individuals and companies in class action lawsuits alleging violations of federal securities laws; individuals and companies in investigations commenced by the SEC, CFTC, Department of Justice, state attorneys general and Congress; and The Bank of New York Mellon in all aspects of litigation and SEC and CFTC investigations relating to the bankruptcy of Sentinel Management Group.

Ms Waldman was recently named a Rising Star by the *New York Law Journal*. She is also a recipient of the Legal Aid Society's 2018 Pro Bono Publico Award for outstanding service.

Michael Wang
Clifford Chance

Michael Wang is a senior associate in Clifford Chance's litigation and dispute resolution practice. Admitted in Hong Kong in 2012, Michael is a native Mandarin speaker and is fluent in Cantonese.

Michael advises on a broad range of contentious regulatory matters and complex banking and commercial litigation. He regularly advises banks, investment funds, brokerages, asset managers and listed companies in a wide range of regulatory investigations and compliance

issues, including market misconduct, sponsor liability, algorithmic trading and reporting failures. Michael also advises and represents banks and high net worth individuals in a number of high-profile court and tribunal hearings, both local and cross-border, involving mis-selling of structured products and general commercial disputes.

Holly Ware
Slaughter and May

Holly Ware, a partner in Slaughter and May's dispute resolution group, has a broad practice that includes litigation and contentious regulatory and criminal investigations.

She has cross-jurisdictional investigation experience involving both regulatory and prosecuting authorities, including the LIBOR investigations and others relating to bribery and corruption, market abuse, money laundering and data breaches.

Karen Werner
Bofill Mir & Alvarez Jana

Karen Werner is a litigation partner at Chilean law firm Bofill Mir & Alvarez Jana. Mrs Werner studied law at the Catholic University of Chile, where she graduated *magna cum laude*. Ms Werner obtained an LLM from the Columbia Law School in New York (2017), graduating with honours as a Harlan Fiske Stone Scholar.

Mair Williams
Latham & Watkins

Mair Williams' practice focuses on white-collar defence. She has considerable trial experience having started her career as a criminal barrister in chambers, as well as experience in investigations, representing companies and individuals before regulators and prosecuting bodies, and developing compliance policies and practices for international clients.

In addition to her white-collar work, Ms Williams has experience in all manner of complex commercial litigation and has represented clients at every stage from initial pleadings through to trial and appeal.

Ms Williams has conducted a range of internal investigations including an investigation of a financial services firm following a leak of confidential information to the media and an investigation on behalf of a private pension scheme following allegations made by a whistleblower. Her diverse range of representative experience includes representing a director in an investigation by the Financial Reporting Council into discrepancies with annual accounts of a FTSE 250 company and representing a publicly listed investment firm in investigations by the Financial Conduct Authority and Serious Fraud Office.

Ms Williams has an active *pro bono* practice focused on representing individuals in the criminal justice system and providing legal advice to charities and NGOs.

Milton L Williams
Walden Macht & Haran LLP

Milt Williams' practice focuses on white-collar criminal and regulatory matters, employment law, litigation and advisory work representing corporations, and complex commercial litigation. He has litigated discrimination claims, Dodd-Frank and Sarbanes-Oxley retaliation claims, and SEC and IRS whistleblower claims on behalf of employees, and he has tried over 55 cases (both civil and criminal) to verdict. Before joining Walden Macht & Haran, Milt served as Deputy General Counsel and Chief Compliance Officer at Time Inc, where his responsibilities included compliance, the Foreign Corrupt Practices Act, OFAC, and Sarbanes-Oxley, as well as intellectual property, privacy, data security, and other cutting edge areas. At Time Inc, Milt actively litigated a variety of employment law matters on behalf of the company concerning race, age and gender discrimination, and independent contractor litigation. In 2013, Milt was appointed co-chair of the Moreland Commission to investigate public corruption. Earlier in his career, Milt served as an Assistant US Attorney in the US Attorney's Office (USAO) for the SDNY. His last assigned unit in the USAO was the Securities and Commodities Fraud Force. He was also an Assistant District Attorney in the Manhattan District Attorney's Office. Milt is a graduate of Amherst College and the University of Michigan Law School in Ann Arbor.

Nicholas Williams
Freshfields Bruckhaus Deringer

Nick Williams is a partner within Freshfields' dispute resolution practice in London and a member of the corporate crime group. As well as handling a broad range of large-scale, multi-jurisdictional commercial disputes, Nick has advised on a range of internal corporate, regulatory and criminal investigations (including a number of investigations by the SFO) for major corporate clients, including in the professional services, retail and pharmaceuticals sectors.

Alison Wilson
Linklaters LLP

Alison Wilson is a contentious regulatory partner at Linklaters in London. She advises market-leading financial institutions, particularly in the retail bank sector, on their most significant FCA enforcement investigations, as well as on a range of internal investigations. She routinely advises firms on their investigation of whistleblowing concerns, including in an FCA enforcement context. She also has experience advising clients under investigation by the SFO and overseas enforcement agencies. Alison's contentious regulatory experience includes pre-enforcement work, often helping clients through section 166 Financial Services and Markets Act reviews, thematic reviews and FCA executive procedures.

Alison was listed as one of *Global Investigations Review*'s 40 under 40 investigations lawyers in 2017, as well as being included as a Rising Star in Litigation in *Legal Week*'s 2016 list.

Alison's extensive bank sector knowledge has been supplemented by three bank secondments.

Kyle Wombolt
Herbert Smith Freehills

Kyle Wombolt is the global head of Herbert Smith Freehills' corporate crime and investigations practice. He has been described by clients as 'one of the cornerstones of investigations work in Asia' and 'an exceptional lawyer'. Based in Hong Kong, Kyle has 20 years' experience in Asia and has led investigations and compliance projects in more than 40 countries worldwide. He focuses on multi-jurisdictional anti-corruption, regulatory, fraud and accounting investigations, as well as trade and sanctions issues involving multinational and major regional corporates. He has extensive experience in dealing with a broad group of government agencies and regulators in key jurisdictions in Asia, Europe, Australia and the United States.

Kyle also has a diverse range of experience in implementing anti-corruption compliance programmes for a broad range of clients, including investment banks and other financial institutions and multinational companies. He regularly advises clients on corruption risks associated with a wide range of transactions, including initial public offerings, mergers and acquisitions, and joint ventures.

Kyle is admitted to practise in Hong Kong, California and New York, and is a registered foreign lawyer in England and Wales.

William Wong
Clifford Chance

William Wong is a Hong-Kong based consultant in Clifford Chance's litigation and dispute resolution practice. He is admitted in Hong Kong, and England and Wales, and he has more than 10 years of experience in banking litigation, white-collar crime and all aspects of contentious regulatory work, and he regularly advises a broad range of institutional clients (investment banks, private banks, insurance companies, hedge funds and asset managers) and individual clients (senior executives of listed corporations and financial institutions) in local and cross-border regulatory investigations. He also advises on commercial litigation and employment-related matters from time to time.

Before joining Clifford Chance, William had held in-house positions at two bulge-bracket investment banks, advising on their regulatory and compliance issues and internal investigations. With his in-house experience and trilingual capability, William is a popular counsel of choice, particularly when clients require first-class advice and Chinese language support.

He is ranked as a Next Generation Lawyer in Hong Kong for dispute resolution in the 2017 and 2018 editions of *The Legal 500*.

Alistair Wood
Pinsent Masons LLP

Alistair Wood is a solicitor at Pinsent Masons LLP and a member of the international white-collar crime, investigation and compliance team. He specialises in the conduct of investigations, self-reporting and anti-bribery compliance.

Matthew Worby
Jenner & Block London LLP

Matthew Worby is an associate in Jenner & Block's investigations, compliance and defence practice group. Matthew has experience of representing both international corporates in investigations and defending individuals against prosecution by the SFO.

Zaneta Wykowska
Ropes & Gray LLP

Zaneta Wykowska is an associate at Ropes & Gray in London, who frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Wendy Wysong
Clifford Chance

Wendy Wysong leads Clifford Chance's Asia-Pacific anti-corruption and trade controls practice, maintaining offices in Hong Kong and Washington, DC. Her practice focuses on regulatory compliance and white-collar defence under international law, including the Foreign Corrupt Practices Act, International Traffic in Arms Regulations, Export Administration Regulations, Office of Foreign Assets Control economic sanctions and US anti-boycott laws, as well as government fraud and public corruption.

As a former Assistant US Attorney in Washington, DC, and the Deputy Assistant Secretary for Export Enforcement, Bureau of Industry and Security, Department of Commerce, Wendy counsels and defends clients based on her unique combination of experience and insight as both a prosecutor and regulator before courts and agencies.

Wendy is ranked in Band One in *Chambers for Corporate Investigations/Anti-Corruption*, and was named a Global Elite Thought Leader by *Who's Who Legal: Investigation*. She and her team received unprecedented dual recognition in 2017 as the Export Controls Law Firm of the Year, USA and the Export Controls/Sanctions Law Firm of the Year, Rest of the World by *World Export Controls Review*. Wendy led and coordinated the international team that represented a Chinese telecommunications company charged with violating US export controls and sanctions, securing the first-ever temporary general licence enabling the company to stay in business during the multi-agency investigation.

Bruce E Yannett
Debevoise & Plimpton LLP

Bruce Yannett is deputy presiding partner of the firm and chair of the white-collar and regulatory defence practice at Debevoise & Plimpton. He focuses on white-collar criminal defence, regulatory enforcement and internal investigations. He represents a broad range of companies, financial institutions and their executives in matters involving securities fraud, accounting fraud, foreign bribery, cybersecurity, insider trading and money laundering. He has extensive experience representing corporations and individuals outside the United States in responding to inquiries and investigations.

Chambers Global 2018 recognises Mr Yannett as a Band 1 practitioner for FCPA matters, and *Chambers USA* 2018 recognises Mr Yannett as a Band 1 practitioner for both white-collar criminal defence and FCPA matters. Clients praise his work as 'excellent' and describe him as a 'very strong communicator and litigator' and a 'leading light in the field', noting that 'he has real gravitas about him', giving him the 'immediate respect of everybody in the room'. In a similar vein, *The Legal 500: United States* calls him a 'superstar', *Lawdragon* recognises him as one of the 500 leading lawyers in America, and *Benchmark Litigation* names him a 'Litigation Star'. Further, in selecting Debevoise as 'Litigation Department of the Year' in 2014, *The American Lawyer* stated that Mr Yannett's work on the groundbreaking Siemens FCPA internal investigation, which spanned 34 countries, and settlement with US and German authorities, 'cemented his credibility with regulators' on subsequent matters.

He is a member of the American Law Institute. Mr Yannett is on the board of advisers for the New York University programme on corporate compliance and enforcement.

Early in his career, Mr Yannett served in the Office of Independent Counsel: Iran/Contra and as an assistant United States attorney.

Steve Young
Association of Corporate Investigators

Steve Young spent 20 years in UK law enforcement with the City of London and Metropolitan Police services investigating economic crime. He specialises in the proactive investigation of banking fraud, money laundering, bribery and corruption. He worked internationally with multiple law enforcement agencies in the United States, Europe and Asia. This was followed by six years as Citigroup EMEA regional director of investigations, and eight years as Barclays' global head of investigations for investment banking and wealth management. At Barclays, he managed a team of corporate investigators who worked globally on all aspects of internal and external economic crime, whistleblowing investigations, regulatory investigations and litigation support. To date, he has 39 years of international economic crime experience in both law enforcement and corporate environments. He speaks frequently on economic crime investigations at legal, corporate and law enforcement events. Steve is currently head of fraud and investigations at Lombard Odier & Co Ltd, based in Geneva and chief executive officer of the Association of Corporate Investigators.

Jerina Zapanti
Anagnostopoulos

Jerina (Gerasimoula) Zapanti is a member of the Athens Bar (2001) and the Hellenic Criminal Bar Association (2007). She has considerable experience in cross-border cases involving fraud, bribery, cartel offences, tax offences and money laundering. She is very active in internal corporate investigations and risk management assessment for national and multi-national corporations.

María Haydée Zegarra
Rebaza, Alcázar & De Las Casas

María Haydée Zegarra leads the labour and employment law practice and has extensive experience in providing legal counselling on personnel hiring and layoffs, collective bargaining, outsourcing of workforce, implementation of internal policies and internal investigations for companies in the fishing, port industry, telecommunications, financial, insurance, agro-industrial and aeronautical sectors.

She has been highlighted by our clients for the preparation of strong defence strategies in relation to judicial processes and administrative inspections thanks to her knowledge of the client's operational know-how and more than 15 years of experience in the labour field.

María Haydée actively participates in training workshops for companies on labour issues, such as employment modalities, management of overtime working, disciplinary sanctions management, employment of foreign employees, among others.

Julie Zorrilla
Navacelle

Julie Zorrilla worked as a trainee in the Directorate of Legal Affairs at the French Ministry of Economic Affairs and Finance in 2012 and was a law clerk to the Paris Court of Appeal in 2011.

During the past few years, Ms Zorrilla has worked on complex cross-border financial and criminal matters (including embargoes, index manipulation and SSA) involving top executives and large foreign and French lending institutions. Ms Zorrilla has also handled large-scale corruption matters, advising on both legal and communication strategies.

Appendix 2

Contributors' Contact Details

Addleshaw Goddard LLP
Milton Gate
60 Chiswell Street
London, EC1Y 4AG
United Kingdom
Tel: +44 20 7606 8855
nichola.peters@addleshawgoddard.com
michelle.dekluyver@addleshawgoddard.com
www.addleshawgoddard.com

Allen & Overy LLP
1101 New York Avenue, NW
Washington, DC 20005
United States
Tel: +1 202 683 3800
Fax: +1 202 683 3999
anthony.mansfield@allenovery.com

1221 Avenue of the Americas
New York, NY 10020
United States
Tel: +1 212 610 6300
Fax: +1 212 610 6399
eugene.ingoglia@allenovery.com

www.allenovery.com

Anagnostopoulos
Patriarchou Ioakeim 6
106 74 Athens
Greece
Tel: +30 210 729 2010
Fax: +30 210 729 2015
ianagnostopoulos@iag.gr
jzapanti@iag.gr
atsagkalidis@iag.gr
www.iag.gr

Association of Corporate Investigators
Kemp House
152-160 City Road
London, EC1V 2NX
Tel: +44 20 3129 8522
admin@my-aci.com
www.my-aci.com

Baker McKenzie LLP
100 New Bridge Street
London, EC4V 6JA
United Kingdom
Tel: +44 20 7919 1000
Fax: +44 20 7919 1999
joanna.ludlam@bakermckenzie.com

452 Fifth Avenue
New York, NY 10018
United States
Tel: +1 212 626 4337
Fax: +1 212 310 1696
william.devaney@bakermckenzie.com

www.bakermckenzie.com

BCL Solicitors LLP
51 Lincoln's Inn Fields
London, WC2A 3LZ
United Kingdom
Tel: +44 20 7430 2277
Fax: +44 20 7430 1101
rsallybanks@bcl.com
aamin@bcl.com
jflynn@bcl.com
www.bcl.com

BDO USA, LLP
100 Park Avenue
New York, NY 10017
United States
Tel: +1 212 885 8379
gpomerantz@bdo.com
nsliger@bdo.com
mbarba@bdo.com
www.bdo.com

Bofill Mir & Alvarez Jana
Avenida Andrés Bello 2711, 8th Floor
Torre Costanera
Las Condes
Santiago 7550611
Chile
Tel: +56 227 577 600
Fax: +56 227 577 813
ajana@bmaj.cl
kwerner@bmaj.cl
www.bmaj.cl

Borden Ladner Gervais LLP
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Suite 3400
Toronto
Ontario, M5H 4E3
Canada
Tel: +1 416 367 6000
Fax: +1 416 367 6749
ghamilton@blg.com
mbarutciski@blg.com
www.blg.com

Brown Rudnick LLP
8 Clifford Street
London, W1S 2LQ
United Kingdom
Tel: +44 20 7851 6000
Fax: +44 20 7851 6100
aamole@brownrudnick.com
www.brownrudnick.com

Brunswick Group LLP
16 Lincoln's Inn Fields
London, WC2A 3ED
United Kingdom
Tel: +44 20 7404 5959
Fax: +44 20 7831 2823
cpotter@brunswickgroup.com

600 Massachusetts Avenue, NW
Suite 350
Washington, DC 20001
United States
Tel: +1 202 393 7337
Fax: +1 202 898 1588
kbailey@brunswickgroup.com

www.brunswickgroup.com

Cadwalader, Wickersham & Taft LLP
700 Sixth Street, NW
Washington, DC 20001
United States
Tel: +1 202 862 2456
jodi.avergun@cwt.com
anne.tompkins@cwt.com
robert.duncan@cwt.com
www.cadwalader.com

700 Sixth Street, NW
Washington, DC 20001
United States
Tel: +1 202 862 2200
Fax: +1 202 862 2400
joseph.moreno@cwt.com

200 Liberty Street
New York, NY 10281
United States
Tel: +1 212 504 6000
Fax: +1 212 504 6666
todd.blanche@cwt.com

www.cadwalader.com

Clifford Chance
Clifford Chance
Level 7, 190 St George's Terrace
Perth, WA 6000
Australia
Tel: +61 8 9262 5555
Fax: +61 8 9262 5522
ben.luscombe@cliffordchance.com
kirsten.scott@cliffordchance.com
lara.gotti@cliffordchance.com

Level 16, 1 O'Connell Street
Sydney, NSW 2000
Australia
Tel +61 2 8922 8000
Fax +61 2 8922 8088
tim.grave@cliffordchance.com
angela.pearsall@cliffordchance.com

Clifford Chance
27th Floor, Jardine House
One Connaught Place
Hong Kong
Tel: +852 2825 8888
Fax: +852 2825 8800
donna.wacker@cliffordchance.com
wendy.wysong@cliffordchance.com
anita.lam@cliffordchance.com
william.wong@cliffordchance.com
michael.wang@cliffordchance.com
nicholas.turner@cliffordchance.com

Clifford Chance LLP
10 Upper Bank Street
Canary Wharf
London, E14 5JJ
United Kingdom
Tel: +44 20 7006 1000
Fax: +44 20 7006 5555
luke.tolaini@cliffordchance.com

Clifford Chance US LLP
31 West 52nd Street
New York, NY 10019-6131
United States
Tel: +1 212 878 8000
Fax: +1 212 878 8375
christopher.morvillo@cliffordchance.com
daniel.silver@cliffordchance.com
benjamin.berringer@cliffordchance.com
tara.mcgrath@cliffordchance.com
kaitlyn.ferguson@cliffordchance.com

www.cliffordchance.com

Cloth Fair Chambers
39-40 Cloth Fair
London, EC1A 7NT
United Kingdom
Tel: +44 20 7710 6444
nicholas.purnell@clothfairchambers.com
www.clothfairchambers.com

CMS Cameron McKenna Nabarro Olswang LLP SCP
S-Park, 11–15 Tipografilor Street
B3–B4, 4th Floor
District 1
013714 Bucharest
Romania
Tel: +40 21 40 73 800
Fax: +40 21 40 73 900
gabriel.sidere@cms-cmno.com
www.cms.law

Corker Binning
The Cursitor Building
38 Chancery Lane
London, WC2A 1EN
United Kingdom
Tel: +44 20 7353 6000
Fax: +44 20 7353 6008
jp@corkerbinning.com
as@corkerbinning.com
www.corkerbinning.com

Cravath, Swaine & Moore LLP
825 Eighth Avenue
New York, NY 10019
United States
Tel: +1 212 474 1000
Fax: +1 212 474 3700
jburetta@cravath.com
mlew@cravath.com
cgans@cravath.com
aeisen@cravath.com
www.cravath.com

Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
United States
Tel: +1 212 909 6000
Fax: +1 212 909 6836
beyannett@debevoise.com
dsarratt@debevoise.com
www.debevoise.com

Dechert LLP
1095 Avenue of the Americas
New York, NY 10036-6797
United States
Tel: +1 212 698 3500
Fax: +1 212 698 3599
hector.gonzalez@dechert.com
rebecca.waldman@dechert.com

160 Queen Victoria Street
London, EC4V 4QQ
United Kingdom
Tel: +44 20 7184 7000
Fax: +44 20 7184 7001
caroline.black@dechert.com
lisa.foley@dechert.com

www.dechert.com

DLA Piper LLP
1251 Avenue of the Americas
New York, NY 10020-1104
United States
Tel: +1 212 335 4500
Fax: +1 212 335 4501
john.hillebrecht@dlapiper.com
lisa.tenorio@dlapiper.com
eric.christofferson@dlapiper.com
www.dlapiper.com

Fornari e Associati
Via Chiossetto 18
20122 Milan
Italy
Tel: +39 02 541 222 06
e.difiorino@fornarieassociati.com
www.fornarieassociati.com

Fountain Court Chambers
Fountain Court
Temple
London, EC4Y 9DH
United Kingdom
Tel: +44 20 7583 3335
Fax: +44 20 7353 0329
eld@fountaincourt.co.uk
rl@fountaincourt.co.uk
nxl@fountaincourt.co.uk
to@fountaincourt.co.uk
rjl@fountaincourt.co.uk
ser@fountaincourt.co.uk
www.fountaincourt.co.uk

Freshfields Bruckhaus Deringer
65 Fleet Street
London, EC4Y 1HS
United Kingdom
Tel: +44 20 7936 4000
Fax: +44 20 7832 7001
ali.sallaway@freshfields.com
matthew.bruce@freshfields.com
ben.morgan@freshfields.com
nicholas.williams@freshfields.com
www.freshfields.com

Fox Williams LLP
10 Finsbury Square
London, EC2A 1AF
United Kingdom
Tel: +44 20 7628 2000
Fax: +44 20 7628 2100
jcarlton@foxwilliams.com
sganatra@foxwilliams.com
dmurphy@foxwilliams.com
www.foxwilliams.com

Gleiss Lutz
Taunusanlage 11
60329 Frankfurt
Germany
Tel: +49 69 95514 0
Fax: +49 69 95514 198
eike.bicker@gleisslutz.com
christoph.skoupil@gleisslutz.com
marcus.reischl@gleisslutz.com

Lautenschlagerstrasse 21
70173 Stuttgart
Germany
Tel: +49 711 8997 0
Fax: +49 711 8550 96
christian.steinle@gleisslutz.com

www.gleisslutz.com

Goodwin
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
United States
Tel: +1 212 813 8800
Fax: +1 212 355 3333
rstrassberg@goodwinlaw.com
mspillane@goodwinlaw.com
www.goodwinlaw.com

Gün + Partners
Kore Şehitleri Cad. 17
Zincirlikuyu 34394
Istanbul
Turkey
Tel: + 90 212 354 00 00
Fax: + 90 212 274 20 95
filiz.toprak@gun.av.tr
asena.keser@gun.av.tr
www.gun.av.tr

Herbert Smith Freehills
Herbert Smith Freehills LLP
28th Floor Office Tower
Beijing Yintai Centre
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022
China
Tel: +86 10 6535 5000/5133
Fax: +86 10 6535 5055
mark.chu@hsf.com

Herbert Smith Freehills LLP
38th Floor, Bund Centre
222 Yan An Road East
Shanghai 200002
China
Tel: +86 21 2322 2000
Fax: +86 21 2322 2322
tracey.cui@hsf.com

Herbert Smith Freehills
23rd Floor, Gloucester Tower
15 Queen's Road Central
Hong Kong
Tel: +852 2845 6639
Fax: +852 2845 9099
christine.cuthbert@hsf.com
pamela.kiesselbach@hsf.com
kyle.wombolt@hsf.com

Herbert Smith Freehills LLP
Exchange House
Primrose Street
London, EC2A 2EG
United Kingdom
Tel: +44 20 7466 2580
Fax: +44 20 7374 0888
susannah.cogman@hsf.com
www.herbertsmithfreehills.com

Homburger
Prime Tower
Hardstrasse 201
8005 Zurich
Switzerland
Tel: +41 43 222 10 00
Fax: +41 43 222 15 00
flavio.romerio@homburger.ch
claudio.bazzani@homburger.ch
katrin.ivell@homburger.ch
reto.ferrari-visca@homburger.ch
www.homburger.ch

Jenner & Block
Jenner & Block London LLP
Level 17, Tower 42
25 Old Broad Street
London, EC2N 1HQ
United Kingdom
Tel: +44 330 060 5400
Fax: +44 330 060 5499
khagedorn@jenner.com
rdalling@jenner.com
mworby@jenner.com

Jenner & Block LLP
353 N Clark Street
Chicago, IL 60654
United States
Tel: +1 312 222 9350
glittleton@jenner.com
criely@jenner.com
www.jenner.com

Jones Day
250 Vesey Street
New York, NY 10281-1047
United States
Tel: +1 212 326 3808
Fax: +1 212 755 7306
jloonam@jonesday.com
creardon@jonesday.com
www.jonesday.com

Knoetzl
Herrengasse 1
1010 Vienna
Austria
Tel: +43 1 34 34 000 200
Fax: +43 1 34 34 000 999
bettina.knoetzl@knoetzl.com
thomas.voppichler@knoetzl.com
www.knoetzl.com

Kingsley Napley LLP
Knights Quarter
14 St John's Lane
London, EC1M 4AJ
United Kingdom
Tel: +44 20 7814 1200
Fax: +44 20 7490 2288
cday@kingsleynapley.co.uk
lhodges@kingsleynapley.co.uk
www.kingsleynapley.co.uk

Latham & Watkins
99 Bishopsgate
London, EC2M 3XF
United Kingdom
Tel: +44 20 7710 3001
stuart.alford.qc@lw.com
gail.crawford@lw.com
hayley.pizzey@lw.com
mair.williams@lw.com

885 Third Avenue
New York, NY 10022-4834
United States
Tel: +1 212 906 1330
serrin.turner@lw.com

505 Montgomery Street
Suite 2000
San Francisco, CA 94111-6538
United States
Tel: +1 415 395 8040
max.mazzelli@lw.com

www.lw.com

Law Offices of Panag and Babu
No. 82, First Floor
Phase III, Okhla Industrial Estate
New Delhi, 110020
India
Tel: +91 011 49996 800
sherbir@pblawoffices.com
tanya.ganguli@pblawoffices.com
lavanyaa.chopra@pblawoffices.com
www.pblawoffices.com

Linklaters LLP
One Silk Street
London, EC2Y 8HQ
United Kingdom
Tel: +44 20 7456 2000
Fax: +44 20 7456 2222
jillian.naylor@linklaters.com
alison.wilson@linklaters.com
sinead.casey@linklaters.com
elly.proudlock@linklaters.com
www.linklaters.com

Marval O'Farrell & Mairal
Avenida Leandro N. Alem 882
(C1001AAQ) Buenos Aires
Argentina
Tel: +54 11 4310 0100
Fax: +54 11 4310 0200
pse@marval.com
glo@marval.com
mls@marval.com
www.marval.com

Matheson
70 Sir John Rogerson's Quay
Dublin 2
Ireland
Tel: +353 1 232 2000
Fax: +353 1 232 3333
claire.mcloughlin@matheson.com
karen.reynolds@matheson.com
ciara.dunny@matheson.com
www.matheson.com

Matrix Chambers
Griffin Building
Gray's Inn
London, WC1R 5LN
United Kingdom
Tel: +44 20 7404 3447
Fax: +44 20 7404 3448
edwardcraven@matrixlaw.co.uk
alexbailin@matrixlaw.co.uk
www.matrixlaw.co.uk

Miller & Chevalier Chartered
900 16th Street NW
Washington, DC 20006
United States
Tel: +1 202 626 5800
Fax: +1 202 626 5801
totoole@milchev.com
wbarry@milchev.com
mlaporte@milchev.com
www.millerchevalier.com

Navacelle
60 rue Saint-Lazare
75009 Paris
France
Tel: +33 1 48 78 76 78
Fax: +33 9 81 70 49 00
sdenavacelle@navacellelaw.com
sdossantos@navacellelaw.com
jzorrilla@navacellelaw.com
cduverne@navacellelaw.com
www.navacellelaw.com

Nokia Corporation
3 Sheldon Square
Paddington
London, W2 6PY
United Kingdom
femi.thomas@nokia.com
Tel: +44 7785 399 642
tapan.debnath@nokia.com
Tel: +44 7342 089 528
www.nokia.com

Outer Temple Chambers
222 Strand
London, WC2R 1BA
United Kingdom
Tel: +44 20 7353 6381
Fax: +44 870 220 3256
michael.bowesqc@outertemple.com
www.outertemple.com

Philippi Prietocarrizosa Ferrero DU & Uría – PPU
Carrera 9 #74-08
Office 105
Bogotá
Colombia
Tel: +571 3268600
Fax: +571 3268610
pamela.alarcon@ppulegal.com
diego.cardona@ppulegal.com
www.ppulegal.com

Pinsent Masons LLP
30 Crown Place
Earl Street
London, EC2A 4ES
United Kingdom
Tel: +44 20 7418 7000
Fax: +44 20 7418 7050
tom.stocker@pinsentmasons.com
neil.mcinnes@pinsentmasons.com
laura.gillespie@pinsentmasons.com
stacy.keen@pinsentmasons.com
olga.tocewicz@pinsentmasons.com
alistair.wood@pinsentmasons.com
rebecca.devaney@pinsentmasons.com
www.pinsentmasons.com

Rajah & Tann Singapore LLP
9 Straits View
Marina One West Tower, #06-07
Singapore 018937
Tel: +65 6232 0260/0590
danny.ong@rajahtann.com
sheila.ng@rajahtann.com
https://sg.rajahtannasia.com

Rebaza, Alcázar & De Las Casas
Av. Víctor Andrés Belaúnde 147
Vía Principal 133, Pisos 2 y 3
Edificio Real Dos
San Isidro
Lima 27
Peru
Tel: +511 442 5100
Fax: +511 442 5100
alberto.rebaza@rebaza-alcazar.com
augusto.loli@rebaza-alcazar.com
hector.gadea@rebaza-alcazar.com
mariahaydee.zegarra@rebaza-alcazar.com
sergio.mattos@rebaza-alcazar.com
www.rebaza-alcazar.com

Reed Smith LLP
1901 Avenue of the Stars
Suite 700
Los Angeles, CA 90067-6078
United States
Tel: +1 310 734 5200
Fax: +1 310 734 5299
fmok@reedsmith.com

10 South Wacker Drive
40th Floor
Chicago, IL 60606-7507
United States
Tel: +1 312 207 1000
Fax: +1 312 207 6400
esussman@reedsmith.com
bbolerjack@reedsmith.com

599 Lexington Avenue
22nd Floor
New York, NY 10022
United States
Tel: +1 212 521 5400
Fax: +1 212 521 5450
jachilles@reedsmith.com

www.reedsmith.com

Ropes & Gray LLP

60 Ludgate Hill
London, EC4M 7AW
United Kingdom
Tel: +44 20 3201 1500
Fax: +44 20 3201 1501
judith.seddon@ropesgray.com
amanda.raad@ropesgray.com
sean.seelinger@ropesgray.com
sarah.lambert-porter@ropesgray.com
chris.stott@ropesgray.com
matthew.burn@ropesgray.com
zaneta.wykowska@ropesgray.com

32nd Floor
191 North Wacker Drive
Chicago, IL 60606
United States
Tel: +1 312 845 1200
Fax: +1 312 845 5500
jaime.feeney@ropesgray.com

Prudential Tower
800 Boylston Street
Boston, MA 02199
United States
Tel: +1 617 951 7000
Fax: +1 617 951 7050
sara.berinhout@ropesgray.com

1211 Avenue of the Americas
New York, NY 10036
United States
Tel: +1 212 596 9600
Fax: +1 212 596 9090
michael.mcgovern@ropesgray.com
meghan.gilliganpalermo@ropesgray.com

2099 Pennsylvania Avenue, NW
Washington, DC 20006-6807
United States
Tel: +1 202 508 4655
Fax: +1 202 508 4650
ama.adams@ropesgray.com

www.ropesgray.com

Russell McVeagh

Level 30, Vero Centre
48 Shortland Street
Auckland 1140
New Zealand
Tel: +64 9 367 8000
Fax +64 9 367 8163
polly.pope@russellmcveagh.com
kylie.dunn@russellmcveagh.com

Level 24, Dimension Data House
157 Lambton Quay
Wellington 6143
New Zealand
Tel: +64 4 499 9555
Fax: +64 4 499 9556
emmeline.rushbrook@russellmcveagh.com

www.russellmcveagh.com

Skadden, Arps, Slate, Meagher & Flom (UK) LLP
40 Bank Street
Canary Wharf
London, E14 5DS
United Kingdom
Tel: +44 20 7519 7000
Fax: +44 20 7519 7070
elizabeth.robertson@skadden.com
www.skadden.com

Slaughter and May
One Bunhill Row
London, EC1Y 8YY
United Kingdom
Tel: +44 20 7600 1200
Fax: +44 20 7090 5000
jonathan.cotton@slaughterandmay.com
holly.ware@slaughterandmay.com
www.slaughterandmay.com

Sofunde Osakwe Ogundipe & Belgore
7th Floor
St Nicholas House
26 Catholic Mission Street
Lafiaji Lagos
Nigeria
Tel: +234 1 462 2502/ 897 2065
Fax: +234 1 462 2501
boogundipe@sooblaw.com
oaogundipe@sooblaw.com
www.sooblaw.com

Sullivan & Cromwell LLP
125 Broad Street
New York, NY 10004-2498
United States
Tel: +1 212 558 4000
Fax: +1 212 558 3588
bourtinn@sullcrom.com
www.sullcrom.com

Trench Rossi Watanabe
Rua Lauro Muller, No. 116, Conj. 2802
Edifício Rio Sul Center
Rio de Janeiro 22290-906
Brazil
Tel: +55 21 2206 4929/4900
felipe.ferenzini@trenchrossi.com

Rua Arq. Olavo Redig de Campos, 105
31º andar
Edifício EZ Towers, Torre A
São Paulo 04711-904
Brazil
Tel: +55 11 3048 6800/5506 3455
heloisa.uelze@trenchrossi.com
joao.gameiro@trenchrossi.com

www.trenchrossi.com

Von Wobeser y Sierra, SC
Paseo de los Tamarindos 60, 4th Floor
Bosques de las Lomas
Cuajimalpa de Morelos
05120 Mexico City
Mexico
Tel: +52 55 5258 1039
Fax: +52 55 5258 1099
dsierra@vwys.com.mx

www.vonwobeserysierra.com

Walden Macht & Haran LLP
One Battery Park Plaza, 34th Floor
New York, NY 10004
United States
Tel: +1 212 335 2030
Fax: +1 212 335 2040
mwilliams@wmhlaw.com
apatel@wmhlaw.com
jgardener@wmhlaw.com
www.wmhlaw.com

Index to Volume I

All references are to section number.

Global Investigations Review

The Practitioner's Guide to Global Investigations

Volume II: Global Investigations around the World

Fourth Edition

Editors
Judith Seddon, Eleanor Davison, Christopher J Morvillo,
Michael Bowes QC, Luke Tolaini, Ama A Adams, Tara McGrath

2020

The Practitioner's Guide to Global Investigations

Fourth Edition

Editors

Judith Seddon

Eleanor Davison

Christopher J Morvillo

Michael Bowes QC

Luke Tolaini

Ama A Adams

Tara McGrath

GIR

Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of November 2019, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: natalie.hacker@lbresearch.com
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-228-2

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

ADDLESHAW GODDARD LLP
ALLEN & OVERY LLP
ANAGNOSTOPOULOS
ASSOCIATION OF CORPORATE INVESTIGATORS
BAKER MCKENZIE LLP
BCL SOLICITORS LLP
BDO USA, LLP
BOFILL MIR & ALVAREZ JANA
BORDEN LADNER GERVAIS LLP
BROWN RUDNICK LLP
BRUNSWICK GROUP LLP
CADWALADER, WICKERSHAM & TAFT LLP
CLIFFORD CHANCE
CLOTH FAIR CHAMBERS
CMS CAMERON MCKENNA NABARRO OLSWANG LLP SCP
CONOR REARDON ESQ
CORKER BINNING
CRAVATH, SWAINE & MOORE LLP
DEBEVOISE & PLIMPTON LLP
DECHERT LLP
DLA PIPER LLP
FORNARI E ASSOCIATI
FOUNTAIN COURT CHAMBERS
FOX WILLIAMS LLP
FRESHFIELDS BRUCKHAUS DERINGER

GLEISS LUTZ

GOODWIN

GÜN + PARTNERS

HERBERT SMITH FREEHILLS LLP

HOMBURGER

JAMES P LOONAM ESQ

JENNER & BLOCK LLP

KINGSLEY NAPLEY LLP

KNOETZL

LATHAM & WATKINS

LAW OFFICES OF PANAG AND BABU

LINKLATERS LLP

MARVAL O'FARRELL & MAIRAL

MATHESON

MATRIX CHAMBERS

MILLER & CHEVALIER CHARTERED

NAVACELLE

OUTER TEMPLE CHAMBERS

PHILIPPI PRIETOCARRIZOSA FERRERO DU & URÍA – PPU

PINSENT MASONS LLP

RAJAH & TANN SINGAPORE LLP

REBAZA, ALCÁZAR & DE LAS CASAS

REED SMITH LLP

ROPES & GRAY LLP

RUSSELL MCVEAGH

SKADDEN, ARPS, SLATE, MEAGHER & FLOM (UK) LLP

SLAUGHTER AND MAY

SOFUNDE OSAKWE OGUNDIPE & BELGORE

SULLIVAN & CROMWELL LLP

TRENCH ROSSI WATANABE

VON WOBESER Y SIERRA, SC

WALDEN MACHT & HARAN LLP

Contents

VOLUME II
GLOBAL INVESTIGATIONS AROUND THE WORLD

Introduction to Volume II

Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams and Tara McGrath[1]

Boards and senior executives have never been more concerned that they or their organisation may come under the scrutiny of enforcement authorities. And with good reason. Recent years have seen an upsurge in confidence among enforcement authorities across the globe, which has manifested and led to increased numbers of investigations, fines of unprecedented orders of magnitude and senior executives facing the much more realistic prospect of investigations concerning their own conduct and, in some cases, prosecution, conviction and imprisonment.

In many jurisdictions, the introduction of new offences and changes to the law of corporate criminal liability have provided enforcement authorities with increased opportunities to pursue criminal investigations and ultimately to prosecute corporate entities. Coupled with this has been the incentivisation of corporates to co-operate with investigations and provide information to assist authorities in pursuing culpable individuals through negotiated settlements. In some jurisdictions, notably the United States, co-operation is an established feature of the enforcement landscape and is regularly used to bring investigations to a pragmatic conclusion without the commercially destructive consequences prosecution of a corporate entity can bring. In others, such as the United Kingdom and France, legislation enabling corporates to conclude investigations short of prosecution is still comparatively young.

The law relating to criminal and regulatory investigations shows no sign of standing still. Law and practice across the globe has changed, often in response to highly publicised scandals. Relationships between enforcement authorities continue to grow closer, and there is a marked trend in politicians, prosecutors and regulators carefully watching the way other jurisdictions choose to combat corporate crime, as they assess the most effective mechanisms

1 Judith Seddon and Ama A Adams are partners at Ropes & Gray LLP; Christopher J Morvillo and Luke Tolaini are partners and Tara McGrath is a senior associate at Clifford Chance; Eleanor Davison is a barrister at Fountain Court Chambers; and Michael Bowes QC is a barrister at Outer Temple Chambers.

to apply in their own national contexts. Recent examples of changes to legislation in terms of either extending corporate criminal liability or legislating for its resolution through deferred prosecution agreements (or both) include significant changes being made in Singapore, Japan, Canada, Australia and Ireland at the time of writing. A similar trend may be observed in the regulatory sphere through the implementation of individual accountability regimes modelled on or drawing from the UK Senior Managers and Certification Regime in, for example, Hong Kong, Australia and Singapore.

All these macro factors, together with important changes to technical local legislation (e.g., the EU General Data Protection Regulation), present numerous, significant challenges to corporates and individuals around the world. They can quickly find themselves the target of fast-moving and far-reaching investigations, whose possible outcomes may vary significantly in different jurisdictions.

In Volume II of this Guide, which now covers 25 jurisdictions, local experts from national jurisdictions respond to a common set of questions designed to identify the local – continually evolving – nuances of law and process that practitioners are likely to encounter in responding to the increasing number of cross-border investigations they face. For the first time, Volume II includes four regional overviews: Asia-Pacific, Europe, Latin America and North America.

Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams, Tara McGrath

December 2019
London, New York and Washington, DC

Part I

Regional Overviews

1

Asia-Pacific Overview

Kyle Wombolt and Pamela Kiesselbach[1]

Introduction

The region has witnessed significant corporate investigations, substantive legal reform and aggressive enforcement in recent years. The Banking Royal Commission in Australia, corporate criminal liability provisions inspired by the UK Bribery Act across several jurisdictions in Asia, and the omnipresent focus of the US Department of Justice (DOJ) on China means that companies in the region face clear business risk. And while the continued impact of the United States cannot be underplayed, national authorities are demonstrating an increasing appetite for investigating and prosecuting large cases themselves. Partly as a result of this, there is a continuing increase in complex, multi-jurisdictional investigations. This highlights a further regional trend – increased co-operation between regulators in different jurisdictions. On a practical level, enhanced information sharing requires a coordinated response by investigated parties to manage competing requests for information, determine appropriate remedial steps and ultimately find solutions to conclude multiple investigations. In a region combining civil law and common law jurisdictions, we also see different approaches to data privacy and legal privilege. This can lead to challenges for corporates and their advisers when conducting internal investigations and responding to external regulatory investigations. We highlight below some of the overarching themes and developments that we have been seeing.

Areas of enforcement risk

Bribery and corruption remain core areas for law enforcement, with domestic and international agencies homing in on conduct in the region. National anti-corruption agencies in Australia, Indonesia, Malaysia and China have all bolstered their powers of investigation and oversight. In tandem, some governments (such as Australia and China) have introduced

1 Kyle Wombolt is a partner and Pamela Kiesselbach is senior consultant (England and Wales) at Herbert Smith Freehills.

more stringent corporate penalties. Regional efforts such as the Guangdong–Hong Kong–Macao co-operation project highlight a focus on multilateralism in combating regional graft. In terms of international enforcement, misconduct in China has long been the subject of more corporate bribery investigations under the US Foreign Corrupt Practices Act than any other jurisdiction. Further, in the past year, the US DOJ has launched its China Initiative. This focuses on Chinese companies' outbound activity and reflects the US's desire to pursue prosecution where Chinese companies' offshore activities affect US national interests.

Money laundering, tax evasion, (accounting) fraud, competition and cybercrime are other key areas for corporate investigations in Asia-Pacific.

Anti-money laundering (AML) and terrorist financing have been under the spotlight, with several evaluations being undertaken by the Financial Action Task Force (e.g., in China and Hong Kong), and visits on the horizon for Japan, Korea and key south-east Asian countries. Many jurisdictions, including Hong Kong, Singapore, Vietnam and India, are ramping up domestic AML legislation and corporate enforcement. The region's focus on money laundering is best highlighted by hydra-styled investigations such as 1MDB,[2] which started in Malaysia but has spread to the highest levels of public office and corporate business globally, including world-famous banks. Governments are pursuing regulatory and criminal actions against financial and other institutions for their failure to implement sufficient controls to monitor global transactions.

Banks, in particular, are subject to increasing scrutiny through audits, examinations, inspections and investigations. In tandem, authorities are increasingly relying on sophisticated technology to identify suspicious payment patterns. A recent example is the Singaporean law enforcement agencies' collaboration with OCBC Bank to quicken financial crime detection. Project Poet (Production Orders: Electronic Transmission) automates data retrieval from the bank such that information that would have taken three months to process will now be available to law enforcement agencies within one or two working days. Project Poet also makes use of artificial intelligence and data analytics to improve Singapore's anti-money laundering risk management systems.

Tax evasion is another area in which there has been heightened activity in the region. This has been led by the United States under its Foreign Account Tax Compliance Act (FATCA) and the aftermath of its Swiss bank programme, when the US DOJ announced that it would be following funds that are the subject of US tax evasion from Switzerland to financial centres in Asia, such as Hong Kong and Singapore. The pressure on taxpayers and financial institutions has been accelerated and broadened further by the Organisation for Economic Co-operation and Development's Common Reporting Standard. The 'follow the money' initiatives that are being pursued by a number of jurisdictions, including the United States, have highlighted Asian financial centres as targets. The Indonesian tax amnesty – the aim of which was repatriating off-shore funds – is another obvious example, as a vast majority of the funds were located with banks in Singapore. The upshot is further focus on banks in the region, with authorities in India, Australia and New Zealand showing an appetite for reviewing tax-sharing information to root out corporate tax evasion, particularly through multilateral treaties to prevent base erosion and profit shifting.

2 1Malaysia Development Berhad is an insolvent Malaysian strategic development company.

Fraud, particularly tax and accounting fraud, continue to occupy law enforcement too. In one of the most significant recent examples, Punjab National Bank – one of India's largest state-owned banks – reported massive fraudulent activity at its Mumbai branch by junior branch officials issuing fraudulent letters of credit, resulting in fraudulent transactions amounting to nearly US$2 billion.

Cybercrime is now a board-level issue regardless of jurisdiction, but some of the biggest corporate investigations have been in Asia-Pacific. Asia is considered relatively insecure in terms of infrastructure, meaning cyberattacks are more common there. Singapore, one of the leading global digital economies, has become a target, particularly in the health sector. Elsewhere, Toyota Corp suffered a series of data breaches in Australia, Thailand, Vietnam and Japan, while in the Philippines, retailer Cebuana and two fast-food chains, Wendy's and Jollibee, suffered major cyberattacks. In response, domestic authorities and regulators have increased compliance and reporting requirements. This turns up the temperature on corporates, who must be ready for internal and external investigations emanating from cybercrime.

A shift from individual to corporate liability

Historically, enforcement agencies in Asia-Pacific have focused on individual criminal liability in the context of public sector bribery, often concentrating on prosecuting the government officials receiving the bribes. However, there have been some clear shifts in focus, demonstrated by legislative changes and statements made by enforcement agencies. The most uniform shift in a number of Asia-Pacific jurisdictions relates to the introduction of corporate criminal liability and accountability of senior management. Thailand, India, Japan, Singapore, Malaysia, Indonesia and China have all introduced legislation making it easier either to attach corporate criminal liability or to penalise companies involved in bribery. Australia has announced a review of corporate criminal responsibility, to be delivered in 2020. India, Indonesia, Malaysia and Thailand were all inspired by the UK Bribery Act section 7 corporate offence in crafting their own legislation. In simple terms, under these often still fairly new rules, companies may be held criminally liable if their employees or agents or otherwise 'associated persons' commit bribery or other criminal offences while acting on behalf, or for the benefit, of the company. As is the case under the UK Bribery Act, these rules take into account whether a company had adequate procedures in place to prevent the criminal offence when determining the company's liability. While some provisions are limited to bribery offences (e.g., in Malaysia and India), others are more broadly drafted to cover other criminal offences as well (e.g., in Indonesia). On the other hand, the new corporate criminal liability offence recently introduced in Vietnam covers tax evasion and money laundering offences and does not extend to bribery offences.

The corporate liability offences plug gaps in domestic regimes, give law enforcement and regulators greater powers, and ease the requirement of meeting the difficult threshold of showing involvement of the 'directing mind and will' of the company to establish corporate liability. Critically, there is increasing pressure on companies to put adequate procedures and controls in place to prevent bribery if they wish to escape liability for misconduct carried out by employees or agents when acting for the company.

The new corporate liability provisions in Malaysia and India make it clear that they cover foreign entities that carry on their business, or part of their business, in the jurisdiction. Indonesian laws go one step further and provide that a group company, including a

parent or affiliate company, may be held criminally liable if it is considered to be involved in the bribery. As a result, companies operating in the region should ensure that appropriate internal control measures are in place or re-evaluate their measures so that they comply with relevant domestic guidelines. The increased corporate exposure has also resulted in investors and, in some instances, lenders conducting heightened compliance-related due diligence on local companies before entering into a merger or a joint venture, or making an investment to gauge and manage their exposure.

Senior managers are also facing enhanced exposure to liability, putting their companies under additional compliance risk. A Senior Managers Regime, similar to the UK's Senior Managers' and Certification Regime, has been introduced in Hong Kong and Singapore to enable the financial sector to improve the individual accountability of senior managers. Anti-bribery provisions in Malaysian, Indian and Indonesian laws potentially extend criminal liability to senior management. This means that senior managers may be held liable for bribery committed under their watch when they are seen to have either proactively authorised or at least known of, and acquiesced in, bribery. Although largely untested at this stage, there is a risk that liability may be inferred when there is a suspicion of bribery and a senior manager does nothing to stop the bribery or turns a blind eye to clear indications of bribery. Indonesian law potentially goes further, in that senior management may be held responsible for wrongdoing by employees or agents acting on behalf of a company simply based upon their status.

Other trend shifts relate to broadening the focus to cover private sector bribery and supply-side bribery to an increasing extent. Notable illustrations of the former are the recent introduction of a private sector bribery offence in Vietnam and the fact that around 70 to 80 per cent of bribery-related prosecutions in Singapore and Hong Kong relate to incidents within the private sector. Although public sector bribery is still traditionally considered to attract a higher level of enforcement risk, it is important not to lose sight of the criminality of private sector bribery. In jurisdictions that still 'only' provide for prohibitions on public sector bribery (e.g., India and Indonesia), the scope of who may be considered a 'public official' is often extended. Further, recent legislative changes in India have introduced a supply-side bribery offence and officials at Indonesia's anti-graft body, the Corruption Eradication Commission (KPK), have been issuing statements indicating that they intend to focus more on the givers of bribes and not just on the public officials receiving the bribes.

Culture

Culture has become a central tenet of –– and compliance imperative for – corporate investigations in the region. Banks in particular have been facing a culture and conduct storm. The Banking Royal Commission in Australia best illustrates the role of corporate culture at the meso (organisation) and macro (industry) levels.

With most jurisdictions moving to disclosure-driven, risk-based systems, an assessment of corporate culture involves a top-down review to assess the readiness of a company to limit the occurrence of misconduct and its reaction to it once on notice. A failing corporate culture can be evidenced by any of the following: a lack of corporate policies and training, poor tone from the top, turning a blind eye, and express or tacit authorisation of poor conduct.

UK Bribery Act-inspired legislation in certain jurisdictions, particularly those with adequate procedures defences, highlights the growing relevance of corporate culture in Asia.

Further, corporate culture continues to affect enforcement outcomes. For example, the US DOJ Criminal Division's updated Guidance on the Evaluation of Corporate Compliance Programs helps to benchmark the effectiveness of a company's compliance programme. The Guidance assists US authorities with decisions when conducting an investigation, determining whether to bring charges or negotiating pleas or other arrangements. Whether in the United States, Asia-Pacific or elsewhere, the Guidance sets out useful prompts for a best practice compliance framework. Given the propensity of regulators to borrow from each other's procedures and practices, it will also be of interest to companies subject to regulatory scrutiny, investigation or enforcement outside the United States, as a benchmark for appropriate remediation and resolution.

Guidance was also recently issued by the Prime Minister's Department in Malaysia setting out anti-corruption programmes and procedures to be adopted by companies doing business in Malaysia. The guidance (which is similar to guidance issued in the United Kingdom under the Bribery Act 2010) describes an effective, risk-based compliance programme that minimises the risk of misconduct occurring and, where it does occur, mitigates the potential consequences for the company.

Information-sharing and multi-jurisdictional investigations

It is rare for an allegation into corporate misconduct to remain a domestic affair, such is the global nature of today's commerce and communication. Regulators are ramping up cross-border co-operation and resolutions in response. Some very high-profile corporate investigations demonstrate how concurrent multi-jurisdictional investigations are now the norm. It is noteworthy in this context that cross-border information-sharing between authorities is often informal and will not always follow formal and time-consuming procedures under mutual legal assistance treaties.

The *Rolls-Royce* settlement covered allegations that Rolls-Royce bribed officials in multiple countries for a period of more than 20 years. The British company's alleged bribery of Garuda Airlines and other Indonesian officials was covered in the £671 million settlement Rolls-Royce reached with the UK's Serious Fraud Office (SFO), the US DOJ and Brazil's Federal Prosecution Service in January 2017. The KPK in Indonesia has been questioning individuals at Garuda, and in August 2019 arrested Garuda's former president, Emirsyah Satar, who stands accused of accepting several illicit payments totalling €1.2 million (US$1.5 million) and other items worth US$2 million. The KPK has charged him with money laundering and will take forward his prosecution, while also pursuing related individuals. Meanwhile, Garuda is suing Rolls-Royce for compensation in the Indonesian courts. More recently, Indian authorities, including the Central Bureau of Investigation, have also opened an investigation into the use by Rolls-Royce of third-party intermediaries to win contracts.

GlaxoSmithKline plc (GSK) is another famous example of a global brand being caught up in bribery in Asia, leading to investigations and charges in multiple jurisdictions. Between 2004 and 2010, GSK's sales teams in China were alleged to have bribed doctors to prescribe GSK products. A Chinese court fined GSK China a record 3 billion yuan (US$492 million) for bribery in 2014. The former head of GSK China and four other former GSK senior executives were also found guilty, and GSK China's financial compliance and legal departments were found to have been complicit. Related international investigations have been carried out in the United States by the DOJ and the Securities Exchange Commission (SEC)

for potential violations of the Foreign Corrupt Practices Act, and in the United Kingdom by the SFO for possible breaches of the Bribery Act. The US investigation ended in a settlement in October 2016, with GSK paying the US SEC a US$20 million civil fine. The DOJ and the SFO later declined to prosecute.

Privilege and data privacy: complexities in Asia-Pacific

With a mixture of common law and civil law jurisdictions, law enforcement agencies and regulators in Asia-Pacific adopt very different approaches to legal professional privilege and data protection. For example, China, Japan, Korea, Indonesia, Thailand and Vietnam do not recognise legal privilege, but lawyers owe duties of confidentiality over documents provided to them by their clients. However, this can be overridden by authorities in investigations.

In contrast, common law jurisdictions such as Hong Kong, Singapore, Malaysia, India, Australia and New Zealand all recognise legal privilege to a greater or lesser extent. In general, internal investigation notes and investigation reports produced in the context of corporate investigations may be covered by legal privilege and protected from disclosure in common law jurisdictions, depending on the extent of involvement of either internal or external lawyers in the investigation process. In the same vein, there is a basis for pushing back against seizure of privileged material during dawn raids or other inspections by authorities and regulators. This does not apply in civil law jurisdictions, meaning that in cross-border investigations, the approach of authorities and regulators on the question of legal privilege can be diametrically opposed. Corporates and their lawyers will often try to assert legal privilege in civil law jurisdictions, expecting it to be claimed as part of a broader regional investigation in which common law jurisdictions are also involved. However, this will not prevent documents and data being seized or handed over to authorities and regulators in civil law jurisdictions. Such bodies could potentially then share the evidence with authorities and regulators overseas, resulting in a broader loss of privilege protection.

A related issue is data privacy. In the context of cross-border investigations, the extent to which Asian countries restrict data transfers off-shore varies. India, for example, has no specific legislation covering data protection, and provisions on international data transfers in its proposed (draft) Data Protection Bill are expected to be watered down before it is brought into force. New Zealand is also in the process of bolstering its existing data privacy regime. In contrast, China and Korea, for example, already impose very strict data protection requirements. In China, state secrets laws are usually also engaged, preventing the transfer off-shore of documents that may contain politically sensitive information. In practice, most multinational companies in the region tend to seek employee consent to data use and transfer at the on-boarding stage. However, these may not suffice under local laws, which should always be checked.

The extraterritorial nature of the EU General Data Protection Regulation (GDPR) adds a further potential layer of complexity for corporates operating in Asia-Pacific, since many have branches or processing operations within the European Union. The mega-fines issued recently pursuant to the GDPR are a sober warning to all companies, regardless of location. Ensuring that the processing of data complies with the GDPR, where it applies, is a commercial imperative. In the context of investigations, the GDPR, in line with most domestic data privacy laws, gives authorities the right to receive from investigated companies or other authorities, personal data in the context of regulatory criminal investigations. In

internal investigations, a combination of processing conditions under the GDPR and local data privacy law exemptions and derogations (where applicable) will dictate whether transfers are permissible. This needs to be assessed in each individual case and will remain an area of interest in investigations in the region.

Increased pressure and incentives to co-operate

Asia-Pacific has seen the emergence of corporate settlement regimes in recent years. As seen in the United States and the United Kingdom, deferred prosecution agreement (DPA) regimes create strong incentives for self-disclosure by companies, and those that disclose, co-operate and remediate may avoid prosecution in favour of fines or monitorship.

These voluntary self-reporting regimes are to be differentiated from statutory reporting obligations that exist under many anti-money laundering laws across the region and in some jurisdictions in relation to some predicate offences. Anti-money laundering laws may require the reporting of a suspicion of criminal proceeds flowing from a criminal act such as bribery. Laws in Malaysia and Vietnam go further and require the reporting of a bribery offence (regardless of whether the offence has resulted in criminal proceeds). The failure to report will often in itself constitute a criminal offence, and reporting obligations will need to be kept in mind whenever potential criminal misconduct is being investigated.

In anticipation of a new DPA regime in Australia, various authorities, including the Federal Police, have issued self-reporting guidelines to assist corporations that wish to self-report actual or suspected foreign bribery offences. Self-reporting (together with co-operation) will be taken into account both in deciding whether to prosecute and, if prosecuted, as a mitigating factor during sentencing. Early guilty pleas by a company may also result in significant reductions in sentencing. Federal DPA legislation is expected to be introduced in Australia in late 2019. New Zealand's regime falls short of a DPA system, but certain agencies, such as the Financial Markets Authority, may obtain 'enforceable undertakings' that help companies avoid prosecution.

Financial regulators such as the Securities and Futures Commission in Hong Kong, in limited circumstances, entertain negotiation resulting in reduced sanctions or declinations to prosecute. India and China have no non-prosecution agreement or DPA system, although in practice, self-reporting and co-operation may be taken into account in mitigation.

DPAs were introduced in Singapore in late 2018. This followed on the heels of the first multi-jurisdictional DPA entered into with the US DOJ involving Singapore authorities. This was a rare example of a Singapore company being penalised by Singapore authorities under national anti-bribery laws for bribery committed abroad. It was by far the highest penalty levied against a Singapore company and was the first DPA involving co-operation between the Brazilian, Singapore and US authorities. Singapore's DPA regime is similar to the UK's except that Singapore DPAs cover a more limited range of criminal offences and Singapore prosecutors are not required to issue guidelines on when a DPA is appropriate and on what 'discounts' may be offered in the case of self-reporting, meaning that prosecutors retain maximum flexibility. Further, the Singapore DPA regime is unusual in that, unlike other jurisdictions with a DPA regime, Singapore has not yet introduced a corporate bribery offence, which means that there is likely to be less of an incentive to self-report and seek a DPA.

In Japan, a plea bargaining regime was introduced in June 2018. Unlike DPAs, this applies to individuals, not companies. Suspects and defendants will be rewarded with leniency if they

co-operate by providing information or evidence in resolving another person's crimes or by giving depositions against partners in crime (including corporates). This is likely to lead to an uptick in corporate investigations, as individuals become incentivised to inform the authorities about the activities of others, including their employers.

Whistleblowing regimes are a corollary of DPAs; both encourage early notification and co-operation. Australia has introduced new whistleblower protection laws, which came into effect on 1 July 2019. These strengthen protection and compensation for whistleblowers and impose on regulated companies the requirement to implement corporate whistleblowing frameworks, including confidentiality and non-retaliation provisions. India passed a Whistleblowing Act in 2014 but it has not yet been brought into effect. Japan is consulting on expanding whistleblower protections as current laws have been criticised as a toothless tiger, owing to the lack of sanctions on companies that treat whistleblowers unfairly. Hong Kong and Singapore still lack dedicated whistleblower legislation, but do have provisions in a patchwork of laws and regulatory requirements to protect whistleblowers in certain circumstances. China's whistleblower legislation goes further than most in the region in including a reward mechanism for whistleblowers who report crimes to people's procuratorates. Various other financial reward schemes are scattered in sector-specific regulations. However, this does not compare to the huge financial incentives and bounties available in the United States under the Dodd-Frank Act. Regardless of incentives and protections, in Asia at least, there remain cultural and hierarchical norms that often militate against blowing the whistle and reporting up. These may mean that new legislation has limited traction, but time will tell.

2

Europe Overview

Judith Seddon, Amanda Raad and Chris Stott[1]

Introduction

The European investigations landscape is characterised by a patchwork of varying legislative and regulatory frameworks and enforcement approaches, which are often shaped by past events and current political priorities in particular jurisdictions. These variations and the pace of change mean that cross-border investigations, whether involving multiple European jurisdictions or parallel investigations by enforcement authorities in other regions (or sometimes both), frequently present thorny practical and tactical challenges.

This overview does not seek to duplicate the commentary and analysis set out in many of the chapters in this volume. Rather, it looks at some of the key priorities of enforcement authorities, focusing on anti-bribery and corruption and anti-money laundering, areas where there is particularly significant ongoing activity and in which some authorities are adapting their approaches to make effective use of changes in the law and additions to their toolkits. It also looks ahead to seek to identify the key issues and trends on which those who are subject to investigations around Europe should be focusing.

Areas of enforcement risk

Anti-bribery and corruption

A substantial number of investigations by enforcement authorities have arisen following significant legislative developments introducing corporate offences of failure to prevent bribery, which have extraterritorial effect (such as the UK Bribery Act 2010 (UKBA) and France's Sapin II Law). These legislative developments have been accompanied by new mechanisms enabling criminal investigations involving corporate organisations to be concluded through negotiated settlements. To date in Europe, these mechanisms have been mainly (although not exclusively) used in cases concerning historic bribery and corruption involving corporate

1 Judith Seddon and Amanda Raad are partners and Chris Stott is a senior attorney at Ropes & Gray LLP.

organisations. In the United Kingdom, momentum is building for the corporate 'failure to prevent' offences relating to bribery and the facilitation of tax evasion[2] to be extended to cover economic crime more generally.[3]

Further important changes to anti-bribery and corruption legislation are in progress in other jurisdictions. For example, in Ireland an offence analogous to the UK corporate offence of failure to prevent bribery came into force in July 2018.[4] At the time of writing, this offence has not formed the basis of any publicised enforcement action. In the absence of guidance akin to that published by the UK Ministry of Justice in relation to 'adequate procedures' under the UKBA, there is some remaining uncertainty among corporate organisations and their advisers as to exactly what they need to do to be deemed to have 'taken all reasonable steps and exercised all due diligence' and thereby availed themselves of a defence to the corporate offence. As noted below, it seems that the new corporate offence in Ireland is likely to be followed by the introduction of deferred prosecution agreements (DPAs). Arrangements for investigating and prosecuting bribery and corruption and other corporate crime in Ireland are also being overhauled. Together, these developments may have the effect of increasing the number of investigations in this area. Given the nature of the Irish economy, and in particular its attractiveness to multinational technology and financial services companies, there is potential for these investigations to have significant cross-border elements.

Other significant changes are under way in Poland, where legislation enabling prosecutors to take action against corporate organisations for anti-bribery and corruption and other economic offences is in the course of being introduced. This legislation will increase maximum fines and enable corporate organisations to avoid trials by voluntarily admitting liability.

In jurisdictions where changes have already been made, clearer legislation and high-profile successes where it has been used have buoyed the confidence of authorities and bolstered their resources.[5]

Anti-money laundering

Although approaches and the resources available for investigations vary quite considerably between European jurisdictions, anti-money laundering (AML) remains high on most enforcement authorities' agendas. Some of the highest penalties to have been imposed in recent years have resulted from investigations by the UK's Financial Conduct Authority (FCA) and by France's National Finance Office (PNF) for breaches by major institutions of regulatory requirements and criminal law in relation to their AML systems and controls.

---

2 Namely section 7, UK Bribery Act 2010 and sections 45 and 46, Criminal Finances Act 2017.

3 UK: See, for example, the UK government's call for evidence on corporate liability for economic crime <https://www.gov.uk/government/consultations/corporate-liability-for-economic-crime-call-for-evidence>. The consultation period for this ended on March 2017. The government's response to this consultation is still awaited at the time of writing.

4 Ireland: Criminal Justice (Corporate Offences) Act 2018.

5 For details of the increases in and reorganisation of resources devoted to anti-bribery and corruption investigations and enforcement action in France see, for example, the 2017 Annual Report of the French Anti-Corruption Agency <https://www.agence-francaise-anticorruption.gouv.fr/files/files/AFA_rapportAnnuel2017GB.pdf>. For details of revenue generated by deferred prosecution agreements in the UK, see, for example, the Annual Report and Accounts of the Serious Fraud Office 2018–19 <https://www.sfo.gov.uk/wp-content/uploads/2019/07/SFO-Annual-Report-and-Accounts-2018-2019.pdf>.

The size of fines is not the only notable feature of enforcement activity in this area. Reflecting an increasingly close focus on individual accountability (particularly in financial services, as discussed in more detail below), regulators are showing themselves to be ready and able to pursue individuals whom they consider to have played a part in AML failings.

At the time of writing, enforcement activity in this area is particularly intense in Scandinavia, where regulators and prosecutors are taking action against a number of institutions and individuals in relation to well-publicised AML failings. The uptick in enforcement activity already seen in this part of the region looks set to continue as authorities seek to restore confidence in the robustness of financial crime compliance regulation. Enforcement action in such future cases is likely to be conspicuously more decisive and coordinated and penalties considerably higher than those imposed in past cases. National legislators have signalled their intent clearly. For example, in Denmark, the maximum fines that may be imposed for AML failings have been increased eightfold.[6]

Elsewhere in Europe, some authorities are increasingly exploring how AML compliance provides a template for how firms should comply with their other regulatory obligations. For instance, in the UK the FCA has stated that it expects regulated firms to take steps to prevent rather than simply react to criminal market abuse.[7] In doing so, it has taken rules that have long been a central tenet of AML compliance and applied them to a different section of its financial crime remit.

Increased pressure and incentives to co-operate

In England and Wales, the body of cases in which DPAs have been concluded between the Serious Fraud Office (SFO) and co-operating corporate organisations is slowly growing, although the 20 agreements per year predicted during the passage of the legislation that introduced DPAs still seem some way off.

Notwithstanding recommendations from the Organisation for Economic Co-operation and Development that they should be available across the United Kingdom, the Scottish prosecution authority (the Crown Office and Procurator Fiscal Service (COPFS)) has eschewed the introduction of DPAs and has confirmed that it remains committed to the continued use of civil recovery proceedings in cases where prosecution of corporates is not deemed appropriate.[8] This disparity, in conjunction with the fact that the UKBA applies equally in all parts of the United Kingdom, has led to parallel investigations by the SFO and COPFS in at least one ongoing investigation.

In France, the authorities responsible for investigating and prosecuting financial crime, the French Anti-Corruption Agency (AFA) and the PNF, have now concluded five judicial

6 Denmark: Legislation is not yet published at the time of writing but see government statement and report published by the Danish Financial Services Authority <https://www.dfsa.dk/~/media/Nyhedscenter/2019/Report_on_the_Danish_FSAs_supervision_of_Danske-Bank_as_regards_the_Estonia_case-pdf.pdf?la=en> <https://em.dk/media/10757/english-summary-aml-agreement_september-2018.pdf>.

7 UK: See, for example, Rule 6.1.1 in the Senior Management Arrangements, Systems and Controls section of the Financial Conduct Authority's Handbook and to its Financial Crime Guide <https://www.handbook.fca.org.uk/handbook/SYSC/6/?view=chapter> and <https://www.handbook.fca.org.uk/handbook/FCG/1/?view=chapter>.

8 UK (Scotland): See report by Organisation for Economic Co-operation and Development <www.oecd.org/corruption/anti-bribery/UK-Phase-4-Report-ENG.pdf>. See details of prosecutions and civil settlements to date in Scotland under the UK Bribery Act <https://www.copfs.gov.uk/publications/bribery-act>.

public interest agreements (CJIPs) with companies of various sizes, including one in which global penalties imposed exceeded US$1 billion.

Mechanisms similar to DPAs and CJIPs (or aspects of them) exist in some other jurisdictions around Europe, including Belgium, the Czech Republic, Romania and Slovakia, although these arrangements do not cover corruption offences in all cases, nor is the practice and procedure as clearly set out in these jurisdictions, and there are yet to be any publicised concluded cases of the same magnitude as seen in the United Kingdom and France.

As noted above, it looks likely that Ireland will be the next jurisdiction in which it will be possible for corporate organisations to conclude criminal investigations through negotiated settlements. In August 2019, the Irish Law Reform Commission proposed the adoption of arrangements similar to the UK DPA regime. This would closely follow the entry into force of a new corporate offence of failure to prevent bribery.

Where they are available, authorities' and courts' expectations as to what is expected of co-operating corporate organisations for negotiations to take place, and for a settlement to be agreed and approved, are becoming clearer. In particular, the AFA and the PNF in France and the SFO in the UK (in June and August 2019, respectively) have released guidance that clarifies what they consider amounts to co-operation to create the right conditions for a negotiated settlement to follow.[9] Courts and prosecutors have also provided guidance on whether corporate organisations may claim to be demonstrating required levels of co-operation while maintaining claims to legal professional privilege (where it is available).

Culture and individual accountability

Among the most prominent themes in investigations concerning corporate organisations is the focus on culture, both at the time when alleged misconduct occurred and when any investigation is commenced. The definition of what constitutes 'good culture' is elusive. Authorities, deciding whether to commence, continue and discontinue investigations and selecting which charges to pursue, attach substantial importance to whether they consider alleged conduct (including individuals' conduct outside the workplace) to be indicative of a poor culture.

In some cases, culture is forming the primary basis for enforcement action. In the United Kingdom in 2018–2019, the FCA opened more cases concerned with culture and governance than in any previous year. Its most recent statistics indicate that this type of case now accounts for more than 10 per cent of all active investigations.[10] The FCA is likely to remain a comparatively active authority in relation to these types of investigations, and has reiterated its commitment to pursuing more enforcement action in this area, including against individuals.[11]

---

9 UK: See the Serious Fraud Office's Corporate Co-operation Guidance <https://www.sfo.gov.uk/download/corporate-co-operation-guidance/?wpdmdl=24184>.
France: <https://www.agence-francaise-anticorruption.gouv.fr/files/files/Lignes%20directrices%20PNF%20CJIP.pdf>; <https://www.agence-francaise-anticorruption.gouv.fr/fr/lafa-et-parquet-national-financier-precisent-mise-en-oeuvre-convention-judiciaire-dinteret-public>.

10 UK: See Financial Conduct Authority [FCA] Enforcement annual performance report 2018/19 <https://www.fca.org.uk/publication/corporate/annual-report-2018-19-enforcement-performance.pdf>.

11 UK: See FCA Annual Report and Accounts 2018/19 <https://www.fca.org.uk/publication/annual-reports/annual-report-2018-19.pdf>.

When doing so, it and the Prudential Regulation Authority (PRA) have the benefit of the Senior Managers and Certification Regime (SMCR), which has been in force for banks since 2016 and insurance firms since 2017, and which will be extended to all financial services firms from December 2019. The SMCR in the UK goes further than previous regulatory initiatives directed towards individual accountability. It gives the FCA and the PRA powers to take action against a much broader population of individuals within firms. It also requires firms to document the specific responsibilities of their most senior executives, thus providing the FCA and PRA with clear road maps that may be used to hold those individuals accountable for breaches of regulatory requirements by firms. The FCA is now routinely using the SMCR for this purpose during enforcement investigations. Enforcement authorities around Europe have been watching carefully how the UK regulators are seeking to use these mechanisms to drive up standards of behaviour within the financial services industry by taking dissuasive enforcement action against individuals. It appears likely that similar changes will follow in due course elsewhere in Europe.

The UK regulators are not the only ones to attach particular importance to individual accountability and culture. For example, the SMCR was preceded by amendments to the Banking Code in the Netherlands, including a requirement from 1 April 2015 for bankers to swear an oath or declaration that they will perform their duties to the best of their ability and with integrity.[12] While some commentators have pointed to improvements in standards of individual conduct within Dutch institutions since these reforms were introduced, it has not led to substantial increases in the numbers of investigations or enforcement cases pursued against individuals.

In July 2018, the Central Bank of Ireland released a report produced in conjunction with the Dutch national financial services enforcement authority (De Nederlandsche Bank) based on behaviour and culture reviews of five Ireland-based retail banks.[13] The report's recommendations mirror many of those made by the UK Parliamentary Commission on Banking Standards, from which the SMCR ultimately flowed. They include the introduction of new Conduct Standards and a Senior Executive Accountability Regime, both of which would be similar in most respects to the SMCR. The report also recommends the unification of currently fragmented investigative processes to enable enforcement action to be more effectively and efficiently pursued, particularly against individuals.

Even in countries where enforcement authorities have not explicitly named culture as an enforcement priority, boards are increasingly concerned to demonstrate their commitment to culture. Cases across Europe have shown the substantial reputational damage that can result from allegations of poor cultural practices and the speed at which allegations can cross borders (including into jurisdictions where enforcement authorities are active in this area).

Information sharing and multi-jurisdictional investigations

European investigation and enforcement authorities continue to collaborate actively with one another and with their counterparts globally, using mutual legal assistance and less

12 Netherlands: See details of The Banker's Oath <https://www.tuchtrechtbanken.nl/en/the-bankers-oath>.

13 Ireland: See Central Bank of Ireland report,Behaviour and Culture of Irish Retail Banks, July 2018 <https://www.centralbank.ie/docs/default-source/publications/corporate-reports/behaviour-and-culture-of-the-irish-retail-banks.pdf?sfvrsn=2>.

formal arrangements. There have been particularly noticeable increases in efforts to collaborate across borders in jurisdictions where anti-bribery and corruption legislation has recently been overhauled and where authorities have acquired the ability to enter into global settlements involving overseas enforcement authorities.[14]

Across Europe, traditional boundaries between enforcement authorities' remits are becoming increasingly blurred. Enforcement authorities are having to take an increasingly flexible view of what they are responsible for investigating, which authority should take the lead and how they should most effectively collaborate. Overlaps between the remits of antitrust, data protection and financial services enforcement authorities are becoming increasingly apparent.

Enforcement authorities, conscious of the potential for duplication and delay, are anticipating these overlaps, both within and between jurisdictions. For example, in the United Kingdom, the FCA and the Information Commissioner's Office have in place a detailed memorandum of understanding (most recently updated in February 2019) setting out how they will work together following incidents in which they both have an interest.[15] A particular area where collaboration is required is data privacy. Regulators responsible for this area across Europe are building up their enforcement capabilities following the implementation of the General Data Protection Regulation (GDPR). The body of decided cases in respect of breaches of the GDPR is growing relatively rapidly, and some very significant penalties have been imposed in cases that have also featured close collaboration between national authorities.

Although convictions and other enforcement outcomes in one jurisdiction will commonly be the product of extensive information-sharing between authorities, there are as yet few significant concluded examples of enforcement authorities simultaneously pursuing enforcement cases against the same targets in multiple European jurisdictions. No negotiated settlements in criminal cases entered into by European enforcement authorities have yet involved coordinated settlements in more then one European jurisdiction (although there is at least one case in the pipeline which could involve negotiated settlements in the United Kingdom and France).

EU institutions as enforcement authorities

There have to date been relatively few examples of supranational European authorities (other than the European Commission (EC) in its role as an antitrust enforcement authority) taking overarching enforcement action. That said, there are some signs that frameworks to facilitate a greater number of such cases may develop, both as a response to past incidents in which regulatory arrangements have been found to have been lacking and in an effort to counter perceived growing threats.

14 For example, in France, the National Finance Office [PNF] made 103 requests for mutual legal assistance and extradition to overseas agencies in 2018 (after the introduction of Sapin II) compared with 14 such requests in 2014 – Bilan et Activité 2018 du Parquet National Financier (January 2019) <https://www.tribunal-de-paris.justice.fr/sites/default/files/2019-01/PNF_synthese%202018.pdf>.

15 UK: See 'Memorandum of Understanding between the Information Commissioner and the Financial Conduct Authority' <https://ico.org.uk/media/about-the-ico/documents/2614342/financial-conduct-authority-ico-mou.pdf>.

Investigations in response to AML failings in various Scandinavian institutions provide an example. The investigation by the European Banking Authority (EBA), commenced in February 2019, was concerned with the adequacy of Danish and Estonian regulators' AML supervision and enforcement arrangements, and in particular whether deficiencies in these arrangements amounted to a breach of EU law.[16]

The EBA's investigation did not examine in detail the underlying alleged misconduct by institutions or individuals and was closed in April 2019 without any formal action being taken. Politicians around Europe and the EBA itself have pointed to this investigation as an illustration of the need for its investigative and enforcement powers to be bolstered to enable it more effectively to coordinate action by national authorities and to take more wide-ranging action if those authorities' responses to wrongdoing are not sufficiently robust.

Adding to the EBA's enforcement powers in this way would take time and would require further European legislation. The most effective form for this to take would be a directly applicable regulation imposing uniform powers in all EU Member States. Until now, AML legislation encouraging closer collaboration between national investigation and enforcement authorities has taken the form of successive Money Laundering Directives (which, as they are directly effective instruments requiring transposition by Member States into their national laws, have been implemented in different ways and to different extents).

In some instances, bilateral and multinational arrangements are in place, helping authorities to deploy their resources as effectively and efficiently as possible in cross-border AML investigations. The most recent example, which is also a response to the concerns about previous enforcement arrangements already mentioned, is a formal mechanism to enable Baltic and Nordic AML regulators to exchange information and coordinate enforcement action. There are also increasingly sophisticated mechanisms in place in some jurisdictions to enable information-sharing between private sector organisations and enforcement authorities.[17] However, arrangements are far from uniform across Europe. The extent to which the requirements set out in successive Money Laundering Directives have been effectively transposed, and other provisions relating to cross-border collaboration and resourcing of national authorities have been implemented, varies widely between jurisdictions.

Away from AML enforcement, the EC remains active as an antitrust enforcement authority. Some long-standing themes continue to feature in European antitrust investigations. There are exceptions to rules relating to legal professional privilege (in jurisdictions where it is part of the legal landscape). Leniency provisions often do not dovetail neatly with other regulatory mandatory reporting obligations. There are significant variations in the approaches taken by the EC and national competition authorities. These and other themes mean that European antitrust investigations have to be handled differently from those pursued by other regulators.

In other areas, authorities with a pan-European remit have been active. The European Anti-Fraud Office (OLAF), the division of the EC responsible for investigating fraud against

16 See European Banking Authority press release, 19 February 2019 <https://eba.europa.eu/-/eba-opens-formal-investigation-into-possible-breach-of-union-law-by-the-estonian-and-danish-competent-authorities-regarding-money-laundering-activitie>.

17 In the UK, with effect from October 2017, previously voluntary arrangements enabling information sharing within the private sector and between private sector organisations and enforcement authorities were placed on a statutory footing – section 11, Criminal Finances Act 2017 (which amended Proceeds of Crime Act 2002).

the EU budget and corruption and serious misconduct within EU institutions, has been particularly active in bringing investigations. Its most recent available statistics indicate that it concluded 197 investigations and commenced 215 investigations during 2017 and recommended that national authorities take action to recover more than €3 billion.[18]

Also at the investigative level, Europol has conducted extensive work to seek to coordinate national responses and lay the foundations for possible future multilateral criminal enforcement action in a number of areas, including notably in relation to large-scale cyber attacks.[19]

It seems likely that levels of coordinated pan-European criminal enforcement action will increase in years to come. A new European Public Prosecutor's Office (EPPO) is due to become operational in late 2020. In Member States that have signed up to the arrangements establishing it (which is 22 at the time of writing, with Sweden, Hungary, Denmark, Ireland and Poland having opted out), EPPO will have powers to investigate and prosecute crimes against the EU budget, such as fraud, corruption and tax fraud valued at over €10 million. It will not replace OLAF or other existing investigating and prosecuting authorities (or national enforcement authorities) but will pool experience, adopt a consistent prosecution policy and be able to use streamlined procedures for the exchange of information across borders. In September 2019, Laura Codruța Kövesi, who formerly headed Romania's National Anticorruption Directorate and served as the Romanian prosecutor general, was confirmed as the head of EPPO and Europe's new chief prosecutor. She has indicated a willingness to use EPPO's powers extensively when the agency becomes operational.[20]

Brexit uncertainty

At the time of writing, significant questions remain unanswered as to what the effect of Brexit will be on the mechanisms by which UK authorities work with their counterparts in mainland Europe, especially if no deal is agreed. The withdrawal agreement negotiated between the UK government and the European Union (but which has not been approved by the UK Parliament) does provide for some continuity in relation to existing mechanisms, such as European investigation orders, at least until new arrangements are negotiated. A no-deal situation would mean that authorities would have to fall back on a tangled web of specific agreements. Delays would inevitably follow and practical issues could conceivably flow from the operation of blocking statutes in some jurisdictions (most notably in France and Switzerland).

18 See European Anti-Fraud Office statistics <https://ec.europa.eu/anti-fraud/investigations/fraud-figures_en>.

19 See Europol press release, 18 March 2019 <https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks>.

20 See further details in relation to European Public Prosecutor's Office <https://europa.eu/rapid/press-release_MEMO-17-1551_en.htm> and the appointment of the European Chief Prosecutor <http://www.europarl.europa.eu/news/en/press-room/20190923IPR61749/kovesi-to-become-eu-chief-prosecutor>.

3

Latin America Overview

Pamela Alarcón and Diego Cardona[1]

Introduction: anticompetitive practices, corruption and compliance

There cannot be free competition in corrupted contexts; therefore, the degree of competition in open markets will be distorted because of corrupt practices. The connection between anticompetitive practices and corruption is more evident in public tendering or procurement in public contracts, considering the immense effect these offerings can have on a government's finances. Collusive behaviour, conspiracies or agreements to raise prices, lower the quality of goods or obtain public contracts, cost governments and taxpayers billions of dollars and the consequences can be seen in last year's grand corruption scandals in Latin America. The highest-profile corporate investigations in the region currently are those involving corruption in public contracts and concessions in sectors such as infrastructure, health and public function.

The Organisation for Economic Co-operation and Development (OECD) recognises that the:

> *most common intersection of corruption and anticompetitive conduct occurs in government procurement when bid rigging can be combined with or facilitated by bribery of public officials or unlawful kickbacks. Collusion and corruption are distinct problems within public procurement, yet they may frequently occur in tandem, and have mutually reinforcing effect. Corruption is a big barrier to competition, discouraging genuine competitors from bidding for a contract in cases where they are apprehensive of unfair competition or are unwilling, or unable, to pay bribes.*[2]

1 Pamela Alarcón and Diego Cardona are partners at Philippi Prietocarrizosa Ferrero Du & Uría.

2 Organisation for Economic Co-operation and Development [OECD], 'Fighting bid rigging in public procurement: Report on implementing the OECD Recommendation', 2016, p. 82 <http://www.oecd.org/daf/competition/Fighting-bid-rigging-in-public-procurement-2016-implementation-report.pdf>.

Most Latin American governments have come to recognise the need to promote free competition as a key to achieving growth and development. An appropriate framework for competition has been linked to better performing economics, and consequently business opportunities increase for citizens and the cost of goods and services decrease. By the same token, unilateral acts and agreements that prevent, restrict or hinder free competition injure the economy and society. Therefore, most Latin American countries have been strengthening their competition and antitrust legal framework to fight anticompetitive conduct such as price-fixing, predatory practices, bid rigging and other collusive practices in public tendering. Allowing participants to compete on equal grounds and without barriers has become an essential goal of competition regulations.

This chapter analyses antitrust laws and regulations, and specific provisions for collusion in public tendering in Colombia, Peru and Chile. It discusses internal and government investigations and litigation from a regional perspective.

Legal framework

In general, competition laws in Latin America aim to protect free competition, thereby promoting economic efficiency and consumer welfare. To achieve these goals, national competition regimes in Latin America prohibit anticompetitive practices that hinder free competition in local markets, ultimately affecting the corresponding economic systems. Competition laws typically prohibit both unilateral conduct and anticompetitive agreements, including price-fixing, output restrictions, market allocation and bid rigging, among others. Competition authorities in the region have increasingly turned their enforcement attention to bid rigging in public procurement processes, as this type of conduct typically affects public resources raised by governments for the welfare of society as a whole.

The following analysis focuses on provisions that address collusion in public tendering.

Chile

The Chilean antitrust regulation is contained in Decree Law 211, 1973 (DL 211) and its subsequent amendments. Article 1 of DL 211 stipulates that the objective of the Law is to promote and defend free market competition. In turn, Article 3 establishes a general prohibition against performing or executing, individually or collectively, any act or agreement that prevents, restricts or hinders free competition, or that tends to produce such effects. Such conduct will be sanctioned, without prejudice to the preventive, corrective or prohibitive measures that may be provided in each case.[3]

Regarding collusive practices in public tendering, Article 3(a) of DL 211 prohibits agreements or concerted practices that involve behaviour between competitors that aims to affect the outcome of bidding processes.[4]

Historically, under this regulation, for such practices to be punishable by law, the authorities had to prove that the person or entity in question obtained market power as a result of the conduct. However, in 2016, the regulation was amended, and obtaining market power is no longer a prerequisite for the punishment of anticompetitive conduct.

3 Decree Law 211, 1973, Article 3.

4 Id.

For enforcement of the Chilean antitrust law and regulations, there are two independent bodies. The prosecuting authority is the National Economic Prosecutors Office (FNE), and the authority in charge of preventing and sanctioning anticompetitive conduct is the Antitrust Court (TDLC).

Law No. 19.911.7, 2003 and Law No. 20.361, 2009 regulate most of the FNE's faculties and its relationship with the TDLC. In addition, Law No. 20.361, 2009, Article 8, which modified Article 39 of DL 211, strengthened the FNE's power to fight cartels and other serious competition offences.

Several legal powers of the FNE are established in sections (f), (k), (l) and (m) of Article 39 of DL 211 and include:

> *(f) to request the collaboration of government services and their employees in the exercise of its functions;*
> *(k) to require reports from technical government bodies and hire the services of experts and technicians;*
> *(l) to sign agreements with government services and universities or other (overseas) competition agencies for the purpose of promoting and defending free competition;*
> *(m) to enter into agreements for the transfer of information with other State bodies or electronic interconnection with private parties or overseas agencies.*

Further regulations dictate when the FNE may collect information from private parties and establish that such information can only be gathered in the course of an investigation. Article 43 of DL 211 provides that the FNE's public officials must 'treat all the information or data to which they may have access in the exercise of their tasks and, especially, that information or data obtained as a result of their powers, as confidential'.[5]

Colombia

The current Colombian antitrust regime is marked by the enactment of Law 155, 1959, which was issued before the 1991 National Constitution. Law 155 provides the basic legal standard applying to anticompetitive conduct, agreements and unilateral acts, set forth as a general prohibition against:

> *Any agreements or arrangements that directly or indirectly have as their purpose to limit the production, supply, distribution or consumption of national or foreign raw materials, products, goods or services and, in general, any type of practice and procedure or system tending to limit free competition and to maintain or determine inequitable prices.*[6]

The Colombian antitrust regime was modernised and restructured in 1992 through Decree 2153, which introduced a list of certain specific agreements and unilateral acts that are deemed contrary to free competition, and certain actions constituting abuse of dominance. Under the provisions of Decree 2153, both agreements and unilateral acts that have

5 Decree Law 211, 1973, Article 43.

6 Law 155, 1959, Article 1.

anticompetitive purpose or anticompetitive effects are considered unlawful. The general prohibition under Law 155 is still in force, serving as a catch-all for anticompetitive conduct not otherwise specified under the provisions of Decree 2153.

The Colombian competition regime was further updated with the enactment of Law 1340, 2009, which introduced significant amendments to modernise the free competition protection system and to optimise the tools available for enforcing competition law, notably, substantially increasing the applicable fines for competition violations and introducing a leniency programme, among others.

The Superintendence of Industry and Trade (SIC) is the authority that monitors competition matters and enforces competition laws. The SIC is an administrative body attached to the Ministry of Commerce, Industry and Tourism, which has investigative and sanctioning powers.

Collusion in bidding and tendering processes, including in public tendering, is considered contrary to free competition under Article 47(9) of Decree 2153, which specifically prohibits those agreements 'whose object is the collusion in tenders or contests or those whose effect is the distribution of contract awards, the distribution of contests or the fixing of terms of proposals'.

Moreover, in 2011 bid-rigging in public procurement proceedings was established as a criminal offence by Article 27 of Law 1774, which added Article 410a to Colombia's Criminal Code, prohibiting collusive practices in public tendering, regarding agreements or concerted practices that involve behaviour between competitors with the aim of affecting the outcome of public bidding processes. The Attorney General's Office (the SIC has no criminal law enforcement authority) is in charge of enforcing criminal liability for directors, legal representatives or employees who have taken part in collusive practices in public tendering.

Peru

The main law that governs free competition in Peru is Legislative Decree 1034, 2008 (D. 1034), which enacted the Law of Repression of Anticompetitive Conduct. The Peruvian regulatory framework for the defence of free competition aims to promote economic efficiency in the market, as a means to improve consumer welfare.

In general, the Peruvian competition laws prohibit abuse of dominance, as well as horizontal and (certain) vertical collusive practices.

Article 11 of D. 1034 describes horizontal collusive practices as 'agreements, decisions, recommendations or concerted practices made by competitors, with the purpose or effect of restricting, preventing or distorting free competition'. This provision includes a sample list of types of conduct that can be considered collusive, including efforts to 'agree or coordinate offers, bids, proposals or abstaining from bidding in public or private invitations to tender or contests, or other forms of public procurement, and in public auctions'.

Moreover, horizontal agreements on bids or abstaining from bidding in public bids, tenders or other forms of public procurements or actions are considered as absolute prohibitions under Article 11.2 of D. 1034. Similar to per se violations, agreements under the absolute prohibition standard do not require analysis of competitive effects, only requiring the competition authority to prove the occurrence of the conduct to demonstrate the existence of the infraction.

The absolute prohibition standard is opposed to the relative prohibition standard, which requires the competition authority to demonstrate the existence of the conduct and its potential negative effects within the market.

The Peruvian competition regime is enforced by the National Institute for the Defence of Competition and Protection of Intellectual Property (INDECOPI).

Article 384 of the Peruvian Criminal Code makes it a crime to engage in collusion in public tendering. The most important element in the crime of collusion is defined or known as the concertation (agreement), between a public servant and a private party. The concertation for collusion requires an agreement between the parties to defraud a public entity. Accordingly, under this crime, a simple request or proposal is not sufficient to be punishable within the framework of a criminal process.

The law on collusion in public tendering requires the offender to be an official or public servant. For the existence of an illegal agreement, an interested party within the private sector must participate. The participating private party (known as extraneous) is considered a primary accomplice, and, according to Article 25 of the Peruvian Criminal Code, is sanctioned with the same penalty as the initiator of the crime.

Any agreement that falls within the scope of the crime of collusion must be clandestine and necessarily harm the interests of the state, or cause damage. For this, public servants or officials must violate their functions, prioritising their own interests before those of the state.[7]

Cultural context

In this section, we analyse compliance of antitrust laws that address collusion in public tendering, to identify trends and behavioural patterns within antitrust authorities.

Chile

Since its implementation, the antitrust regime in Chile has been accompanied by a strong legal culture, marked by increased compliance and respect for the law, especially regarding collusive practices in state-contracted bidding. This can be evidenced in the limited number of bid rigging cases persecuted by the Chilean Competition Authority,[8] which led its last bid rigging investigation in 2018 after more than five years of inactive investigations.[9] There is thus a shortage of cases, rather than a disinterest in pursuit from the Chilean authority. Consequently, for the Chilean market, there is a lack of recognisable patterns at this time.

Colombia

In the past decade, the media has taken an increased and sustained interest in cases involving collusive practices in public tendering, helping expose them to the public. Negative opinion surrounding such conduct can be traced back to the 'public procurement carousel',[10] which

7 Supreme Court of Justice of the Republic of Peru (Appeal for Annulment No. 5–2015 – Junín – 16 November 2017).

8 Tribunal de Defensa de la Libre Competencia.

9 *Fiscalía Nacional Económica v. Fresenius Kabi Chile Limitada, Laboratorio Biosano S.A. y Laboratorio Sanderson S.A.* (Case No. 165/2018). The ruling is currently appealed to the Supreme Court and is pending a decision.

10 Superintendence of Industry and Trade, Resolution 54695, 2013: Investigations that were carried out against the 'Nule Group' for their fraudulent participation in different public infrastructure projects.

inspired a significant institutional movement with the aim of protecting public procurement and combating collusive practices. In response to the scandal, the Colombian government promoted the enactment of a new law on corruption in state procurement processes – Law 1471, 2011. It criminalised collusive practices in public tendering and made the Attorney General's Office a critical player in the battle against this type of illicit behaviour. In addition to other administrative and legal efforts, the SIC promoted new institutional projects, including the creation of an Interdisciplinary Group of Collusion in 2012,[11,12] and its relaunch in 2016 as an Elite Group Against Collusive Practices in Public Tendering.[13]

In 2015, the SIC and the Attorney General's Office signed a co-operation agreement to enforce anti-collusive practices in the private sector. This agreement includes the exchange of information and evidence collected, and training programmes for public servants. It also includes a system to post complaints to the Attorney General's Office once the SIC begins an administrative investigation.

Following these efforts, the past decade has seen an increase in the number of investigations carried out by the Colombian competition authority. Between 1992 and 2009, there were some 16 decisions against anticompetitive behaviour relating to collusive practices in public tenders.[14] Between 2010 and 2017, the SIC formally opened 24 investigations into bid rigging in public procurement, imposed sanctions in 13 cases and closed two cases for lack of evidence. These 15 decisions (13 sanctions and 2 closed files) on bid rigging in public procurement amount to approximately 24 per cent of all antitrust cases decided by the SIC during this period.[15] Finally, between January 2018 and May 2019, the competition authority sanctioned 23 market agents for bid rigging in public procurement cases.[16]

Between 2004 and 2018, the SIC's rulings concerning collusive behaviour in public procurement processes tackled some of the most significant corruption scandals in the

11 Superintendence of Industry and Trade 2010–2012 <https://issuu.com/quioscosic/docs/superintendencia_2010_2012/132>.

12 Deisy Galvis-Quintero, 'La colusión como una práctica restrictiva de la competencia que afecta gravemente los procesos de selección de contratistas', 132 Vniversitas, pág. 178 (2016) <http://dx.doi.org/10.11144/Javeriana.vj132.cprc>.

13 'La SIC creará un grupo élite para atacar la colusión en licitaciones públicas', *Diario la República*, 12 November 2016 <https://www.asuntoslegales.com.co/actualidad/la-sic-creara-grupo-elite-para-atacar-la-colusion-en-licitaciones-publicas-2440986>.

14 Camilo Pabón Almanza, 'La libertad de competencia en los procesos de selección objetiva', Universidad Externado de Colombia (2012)

15 Andrés Palacios Lleras, 'La lucha contra los carteles empresariales en la contratación estatal en Colombia', *Latin American Law Review* (N. 03) p. 124 (2019).

16 'Superintendencia ha impuesto multas por más de $111 mil millones por violaciones a la libre competencia entre 2018 y 2019', Superintendence of Industry and Trade <www.sic.gov.co/Superindustria-ha-impuesto-multas-por-mas-de-111-mil-millones-por-violaciones-a-la-libre-competencia-entre-2018-y-2019>.

country.[17] The SIC maintained its focus on investigating and sanctioning collusive practices regarding infrastructure and the provision of services.

In 2018, the SIC formally charged 23 companies for competition law violations relating to hardcore cartel practices in public tendering during 2014 and 2017 (Resolution Order N. 27915). The Resolution indicated that:

- among the alleged cartelists, the parties would determine who would be the bidder or bidders in each contracting process in which they would apply the cartelist or collusive strategy;
- the proponent or bidder who was slated to win the bid would offer the competitors a sum of money or bribe. The SIC established that, in some cases, the bribe payment was made through façade collection accounts that were purportedly for transport services offered;
- the competing bidders who accepted the bribe payment then refrained from improving their offers in the reverse auction. As a result, the bidder slated to win by the cartelists was awarded the contract, after the alleged competitors withdrew from the process; and
- to ensure the highest possible award, the proponent made offers substantially close to the official budget provided by the contracting entity.

In those cases, the SIC ordered copies of the administrative actions to be sent to the Attorney General's Office for criminal investigations for collusive practices in public tendering.

Peru

The Peruvian competition authority investigates and sanctions colluding with private entities, primarily for improper price arrangements and other practices, such as the abuse of the dominant position. Unlike Colombia and other Latin American jurisdictions, collusion cases in public tendering are not a frequent occurrence.

The few cases of collusion in public tenders have involved the purchase and sale of goods and services for state agencies, for instance, haemodialysis services, lubricant containers, and medicinal liquid and gaseous medical oxygen.

These cases occurred during a period of approximately 10 years and affected the capacity of the Peruvian government to service its citizens. This is not surprising as, in Peru, public procurement represents more than 11 per cent of the nation's gross national product.[18]

In 2018, INDECOPI published a document titled 'Guide to Fight Collusion in Public Procurement', which establishes certain parameters and analysis for government officials to identify warning signs for colluding practices within public procurement processes.

In criminal cases, the main problem faced by prosecutors relating to collusive practices is to find evidence to prove the existence of an illegal agreement. In most cases, collusive

17 Superintendence of Industry and Trade: (1) Resolution 54695 of 2013. Investigations that were carried out against the 'Nule Group' for their fraudulent participation in different public infrastructure projects; (2) Resolution 1055, 2009, Resolution 40901, 2012, Resolution 5469, 2013, Resolution 91235, 2013. Investigations conducted against corruption acts in procurement processes by state entities such as Instituto Colombiano de Bienestar Familiar; (3) Resolution 67837, 2018. The *Odebrecht* case refers to collusive practices in procurement contracts and bribe payments amounting to US$28 million by the Brazilian consortium Odebrecht for the awarding of infrastructure projects in the construction of a highway (Ruta del Sol).

18 Garvan, M (2019) 'Indecopi: multas por prácticas colusorias en licitaciones ascienden a S/29 millones', *El Comercio*, 19 March 2019.

agreements are verbal and not written. Therefore, unless one of the accused confesses or the conversation has been recorded, prosecutors face serious problems in obtaining a conviction for collusion.

In some critical cases, prosecutors have reached agreements with the accused in exchange for a confession, which has allowed prosecutors to bring criminal convictions. Nevertheless, these cases are the minority.

When prosecutors fail to find enough evidence to prove the collusive agreement, generally they choose to modify the accusation for the lesser crime of incompatible negotiation,[19] which requires a much lower standard of evidence than collusion (i.e., prosecutors do not need to prove that there was an unlawful agreement, only that the public official had a particular and illegal interest in the contract). However, since the crime of incompatible negotiation is exclusive to public officials, all other persons are excluded from the criminal investigation (i.e., charges are dismissed) and nobody is punished for the illegal conduct.

Administrative sanctions

Chile

The antitrust court may sanction a person who engages in any of the practices described in the 'Legal framework' section, above, namely (1) modifying or terminating those acts or agreements that hinder free competition or (2) ordering the modification or dissolution of partnerships and corporations involved in such conduct, with fines up to the equivalent of 60,000 annual tax units (approximately 35,955 million Chilean pesos).[20]

In the case of the conduct foreseen in Article 3(a) of Decree Law 211 of 1973, the antitrust court may also prohibit colluding private companies from contracting in any capacity with public entities, with autonomous organisms or with institutions, organisations, companies or services in which the state makes contributions, with congress and the judiciary, and from awarding any concession granted by the state, for a period of up to five years.

Colombia

The current competition regime expanded its scope of application with the enactment of Law 1340, 2009. Article 2 of Law 1340 establishes that a natural or legal person who affects, or may affect, the development of economic activities may be subject to sanctions. Under Article 25, a contracting entity that violates free competition rules may be sanctioned, if the crime is proven, with economic fines in favour of the SIC up to 100,000 legal monthly minimum wages (approximately 82 billion Colombian pesos) or, if greater, up to 150 per cent of the profit derived from the conduct displayed by the offender.

In addition to administrative sanctions imposed on economic entities, any natural person who collaborates, facilitates, authorises, executes or tolerates such infractions will be subject

19 Article 399 of the Peruvian Criminal Code: 'A public servant who improperly, directly or indirectly or through a simulated act, becomes interested in his own or for a third party's benefit, in any contract or operation in which he is involved because of his position, will be punished with imprisonment of no less than four or more than six years.'

20 The annual tax unit (UTA) corresponds to the monthly tax unit (UTM) implemented in the last month of the respective commercial year multiplied by 12 or according to the number of months comprising the commercial year. The UTM is a unit of account used in Chile for tax purposes and fines, updated in line with inflation.

to administrative sanctions. In such a case, as per Article 26 of Law 1340, the legal representatives and the senior managers will have to pay fines of up to the equivalent of 2,000 times the legal monthly minimum wage (approximately 1,666,368,000 Colombian pesos) in favour of the SIC.

Peru

If a person engages in any of the practices described in the 'Legal framework' section, above, the INDECOPI may impose the following administrative sanctions.[21]

Economic sanctions

In accordance with D. 1034, INDECOPI may impose economic fines of up to 4,291,601.25 Peruvian soles depending on the severity of the conduct. If the infraction is considered very serious, the fine may exceed the limit set forth by law but is capped at 12 per cent of the gross annual income of the offender.

A related person who promoted or participated in the illegal practice, such as legal representatives, managers or directors of the company, may be sanctioned too. The maximum fines for each representative involved can total 429,069.10 soles.

Corrective measures

In addition to the sanctions imposed for the infringement, INDECOPI at its own discretion may impose corrective measures to restore the competitive process and reverse the effects of the illegal practice.

Corrective measures may include:

- an order to cease illegal activities;
- an obligation to contract with a supplier; and
- the declaration of ineffectiveness or unenforceability of certain anticompetitive clauses or agreements.

The corrective measures that are applied should be based on the degree of impact or harm on the competitive process.

Antitrust compliance programmes

Promoting competition and reducing the risk of corruption and anticompetitive practices in the private sector is a priority of international organisations, such as the OECD. Different guidelines and recommendation documents have been issued to make governments and companies aware of the need to avoid practices that prevent, restrict or hinder free competition. As a result, competition law in many countries has been strengthened, and authorities have been fighting against practices such as collusion.

Currently, it is common to find domestic regulations that protect whistleblowers and enforce leniency programmes, encouraging those with relevant information to come forward, to better enable authorities to conduct investigations of bid rigging in public tendering. In the same way, severe sanctions, including criminal liability and imprisonment, which serve to

21 Legislative Decree 1034, Article 43.

deter would-be wrongdoers, are some of the effective antitrust enforcement policies against collusive behaviour.

Therefore, companies should be aware of the implications and contingencies (legal, reputational and operative) of competition law breaches, mainly those pertaining to collusive practices. For example, if an employee colludes with someone from another company, administrative and criminal sanctions in some jurisdictions could be imposed not only on the individuals – including directors and board members – but also on the corporation or legal person.

In that situation, and if an investigation is started by any competition authority, the employee and the company would be likely to try to seek immunity and the company and the employees may have the same interests; however, the authorities may be interested in granting immunity just for one of them, and to prosecute and sentence the other. In most cases, that 'other' would be the company, considering that it is more attractive for authorities in the region to sanction and impose fines on corporations than individuals. Thus, the authorities use employees as a tool to gather information and evidence on companies' anticompetitive practices.

To avoid this situation, companies should strengthen their compliance programmes, unequivocally condemn price-fixing and collusion, and adopt a zero-tolerance policy towards cartels.

An antitrust compliance programme should include, among other things:

- a clear tone at the top, meaning that the directors and executives commit to abide by the antitrust policies established by the company;
- risk assessments for anticompetitive practices;
- the programme should be implemented effectively and in harmony with policies such as the anti-corruption policy;
- training for employees and executives in identifying antitrust practices;
- the implementation of a channel for complaints and whistleblowing on antitrust issues; and
- guidance or a procedure to ensure information is accurately preserved for later use.

Conclusion

A robust legal culture has emerged in Latin America during the past decade, with increased levels of compliance and respect for the law, especially regarding collusive practices in state-contracting bids. Authorities have more power and legal tools to pursue competitive law infractors. Thus, different kinds of sanctions have been added over the years, including criminal and administrative sanctions for natural and legal persons.

Consequently, companies are more aware of the importance of preventing anticompetitive and antitrust practices that may affect their business and cause damage to customers and the market. Therefore, adopting an antitrust compliance programme in harmony with anti-corruption policies is a useful tool for preventing the commission of such practices and the imposition of fines and sanctions.

4

North America Overview

John D Buretta and Allison Eisen[1]

In late 2018, Canada, Mexico and the United States entered into the aptly named United States-Mexico-Canada Agreement. This Agreement, which imposes obligations on signatory countries to enforce anti-corruption laws, signalled the beginning of a renewed effort to coordinate prosecution efforts across North American borders. The winter of 2018 also saw a convergence at the doorsteps of the United States District Court for the Eastern District of New York of investigative matters spanning the United States, Canada and Mexico. As federal prosecutors were preparing for trial against the famed Mexican drug cartel leader Joaquín Archivaldo Guzmán Loera, also known as El Chapo, other prosecutors in the District were preparing for an extradition battle over Meng Wanzhou, a Chinese national and Huawei executive arrested in Canada on a US federal warrant seeking her extradition to the United States on charges of bank fraud, theft of trade secrets and sanctions evasion. These two matters, among others discussed below, reflect the expanding multilateral nature of enforcement actions in North America, and shed further light on authorities' ability to gather evidence, seek extradition and otherwise coordinate with authorities around the world. A nuanced understanding of the progress, and playbook, on North American corporate enforcement continues to be critical.

The United States-Mexico-Canada Agreement

In late 2018, each country in North America agreed to abide by the United States-Mexico-Canada Agreement, a tripartite treaty that contains an entire chapter on anti-corruption enforcement and compliance.[2] The treaty imposes a range of obligations on signatory countries, effectively to enforce anti-corruption laws and to enact legislation in support of

1 John D Buretta is a partner and Allison Eisen is a member of the litigation department at Cravath, Swaine & Moore LLP.

2 Kara Brockmeyer, Andrew M Levine, Marisa R Taney and Victoria L Recalde, 'NAFTA Replacement Adds Anti-Corruption Provisions', *FCPA Update*, Vol. 10, No. 4 (November 2018).

anti-corruption efforts.[3] The agreement obliges each country to enforce its anti-corruption laws adequately through active prosecution, and provides clear, uniform definitions for terms, such as illicit enrichment and embezzlement.[4] Importantly, the treaty also requires co-operation between the United States, Mexico and Canada, both in sharing resources and experience and in the exchange of information to prevent, detect and deter bribery and corruption.[5] The agreement further extends to promote integrity, honesty and responsibility among public officials of the signatory nations.

Co-operation between the United States and Mexico

Recent cross-border interactions

Conviction of Joaquín Archivaldo Guzmán Loera

In perhaps the most high-profile conviction of a Mexican citizen by the United States in recent memory, in February 2019, Joaquín Archivaldo Guzmán Loera (known as El Chapo) was convicted by a federal jury in Brooklyn of being a principal leader of a continuing criminal enterprise – the Mexican organised crime syndicate known as the *Sinaloa* cartel – on charges that included 26 drug-related violations and one of conspiracy to commit murder.[6] The case of El Chapo was investigated by the US Drug Enforcement Agency (DEA), Immigration and Customs Enforcement and the Federal Bureau of Investigation, working in close consultation with their counterpart authorities in Mexico.[7]

Building the case against El Chapo necessarily required extensive co-operation between authorities in the United States and Mexico. The *Sinaloa* cartel was built on border crossings – cartel members smuggled narcotics from Mexico to wholesale distributors in the United States, then transported billions of illicit dollars back across the border to the Sinaloa area of Mexico – so marshalling evidence required monitoring activity and gathering evidence that spanned a significant geographical range.[8] Throughout the 2000s, officials from both countries worked to build a case against El Chapo, from money laundering to murder charges, and worked for years to pinpoint his exact location.[9] On 22 February 2014, Mexican Marines, with co-operation from US government agencies, arrested El Chapo in Mazatlán, Mexico.[10]

Following the second of El Chapo's two escapes from prison, Mexican officials, sharing intelligence with their US counterparts, together engaged in a manhunt and recaptured

3 United States-Mexico-Canada Agreement, Article 27.

4 Id.

5 Id.

6 US Department of Justice [DOJ] press release (12 February 2019), 'Joaquín "El Chapo" Guzmán, Sinaloa Cartel Leader, Convicted of Running a Continuing Criminal Enterprise and Other Drug-Related Charges' <https://www.justice.gov/usao-edny/pr/joaquin-el-chapo-guzman-sinaloa-cartel-leader-convicted-running-continuing-criminal>.

7 Id.

8 Id.

9 Noah Hurowitz, 'Inside the Trial of El Chapo', *Rolling Stone* (4 November 2018) <https://www.rollingstone.com/culture/culture-features/el-chapo-trial-guzman-brooklyn-court-sinaloa-cartel-751035/>.

10 Randal C Archibold and Ginger Thompson, 'El Chapo, Most-Wanted Drug Lord, Is Captured in Mexico', *The New York Times* (22 February 2014) <https://www.nytimes.com/2014/02/23/world/americas/joaquin-guzman-loera-sinaloa-drug-cartel-leader-is-captured-in-mexico.html>.

him.[11] Despite a history of publicly stating that El Chapo would serve out his sentence in Mexico, the Mexican government subsequently agreed to extradite the cartel leader to the United States to face charges in the Eastern District of New York.[12] The extradition process was not without conflict, however. Mexico outlawed capital punishment in 1975 and has remained steadfast in its refusal to extradite suspects who face the death penalty in the United States.[13] US officials agreed to take the death penalty off the table.[14]

Following his extradition on 19 January 2017, El Chapo was due to stand trial in the United States, which would prove to be another testament to the advanced co-operation between Mexican and US authorities.[15] The evidence presented at El Chapo's trial included testimony from 14 co-operating witnesses, narcotics seizures, weapons, ledgers, text messages, videos, photographs and intercepted phone recordings.[16] The co-operation of witnesses was crucial to building the case against El Chapo. This was particularly true of Vicente Zambada-Niebla, a high-ranking member of the cartel and the son of El Chapo's cartel partner, who was extradited from Mexico to the United States and provided critical testimony about the inner workings of the criminal enterprise.[17]

Following El Chapo's conviction, DEA Acting Administrator Uttam Dhillon stated that the 'success of [the] case is a testament to the strength of [the United States'] relationship with Mexican counterparts'.[18] The strength of this relationship was tested at each stage of the enforcement action, from building the case until conviction at trial.

Past cross-border investigations with Mexico

Although El Chapo's trial and conviction may present the most high-profile example, sustained co-operation between US and Mexican authorities has been evident in corporate investigations during the past few years, and may well expand as Mexico enhances its enforcement tools and efforts.

In December 2016, the US Department of Justice (DOJ) secured guilty pleas from six individuals – four businesspersons employed by Hunt Pan Am, a Houston-based company that provides aircraft maintenance and related services, and two former Mexican government

11 Azam Ahmed, 'El Chapo Case Draws Mexico Closer to U.S.', *The New York Times* (11 January 2016) <https://www.nytimes.com/2016/01/12/world/americas/el-chapo-case-draws-mexico-closer-to-us.html?module=inline>.

12 Azam Ahmed, 'El Chapo. Mexican Drug Kingpin, Is Extradited to U.S.', *The New York Times* (19 January 2017) <https://www.nytimes.com/2017/01/19/world/el-chapo-extradited-mexico.html>.

13 Emily Edmonds-Poli, David A Shirk, 'Extradition as a Tool for International Cooperation: Lessons from the U.S.-Mexico Relationship', *Maryland Journal of International Law,* Volume 33, Issue 1, 215, 226 (2018).

14 Id.

15 Azam Ahmed, 'El Chapo. Mexican Drug Kingpin, Is Extradited to U.S.' – see footnote 12.

16 US DOJ press release, 'Joaquín "El Chapo" Guzmán, Sinaloa Cartel Leader, Convicted of Running a Continuing Criminal Enterprise and Other Drug-Related Charges' – see footnote 6.

17 Jason Meisner, 'Witness Against "El Chapo" Given 15 Years in Prison in Chicago for Key Role in Trafficking Cocaine, Heroin for Cartel', *Chicago Tribune* (30 May 2019) <https://www.chicagotribune.com/news/breaking/ct-met-el-chapo-witness-mexican-cartel-sentencing-20190529-story.htm>.

18 US DOJ press release, 'Joaquín "El Chapo" Guzmán, Sinaloa Cartel Leader, Convicted of Running a Continuing Criminal Enterprise and Other Drug-Related Charges' – see footnote 6.

officials – in a cross-border bribery scheme.[19] The criminal proceeding, which was investigated by US Immigration and Customs Enforcement and the Internal Revenue Service, involved corrupt payments paid to Mexican foreign officials who had responsibility for maintaining Mexico's aircraft, in violation of the US Foreign Corrupt Practices Act. In exchange for the payments (which were made to and from bank accounts in Texas, owned by Hunt Pan Am and the government officials) the government officials awarded contracts for aircraft maintenance and parts to Hunt Pan Am.[20]

The US Securities and Exchange Commission (SEC) has likewise pursued cross-border investigations with Mexico, including in a matter using satellite imagery of land in Mexico as evidence against a Mexican company and its employees. In March 2017, the SEC announced that Mexico's largest homebuilder, Desarrolladora Homex SAB de CV (Homex), 'had agreed to settle charges that it reported fake sales of more than 100,000 homes to boost revenues in its financial statements during a three-year period'.[21] Later that year, the SEC announced related charges against four of the company's former executives, each of whom was a Mexican citizen residing in Mexico.[22]

The SEC alleged that Homex improperly recognised billions of dollars of revenue by 'systematically and fraudulently report[ing] revenue from the sale of tens of thousands of homes annually that it had neither built nor sold'.[23] The SEC's complaint contained satellite images of land in the Mexican state of Guanajuato showing 'housing units which Homex claimed to have built or sold, and for which it had recorded sales and reported revenue', but had clearly not been built.[24] Melissa Hodgman, Associate Director of the SEC's Enforcement Division, noted that the SEC 'used high-resolution satellite imagery and other innovative investigative techniques to unearth that tens of thousands of purportedly built-and-sold homes were, in fact, nothing but bare soil'.[25]

Although Homex is based in Mexico, the SEC claimed jurisdiction because the company's stock had been listed on the New York Stock Exchange.[26] The SEC's announcement of the settlement noted that it 'appreciates the assistance of the Mexican Comisión Nacional Bancaria y de Valores',[27] a regulatory agency that supervises Mexican financial entities. The

19 Foreign Corrupt Practices Clearinghouse, Stanford Law School <http://fcpa.stanford.edu/enforcement-action.html?id=643>.

20 US DOJ, Justice News, 'Four Businessmen and Two Foreign Officials Plead Guilty in Connection with Bribes Paid to Mexican Aviation Officials' (27 December 2016) <https://www.justice.gov/opa/pr/four-businessmen-and-two-foreign-officials-plead-guilty-connection-bribes-paid-mexican>.

21 US Securities and Exchange Commission [SEC], 'SEC Charges Mexico-Based Homebuilder in $3.3 Billion Accounting Fraud' (3 March 2017) <https://www.sec.gov/news/pressrelease/2017-60.htm>.

22 Complaint, *Securities & Exchange Commission v. Gerardo de Nicolas Gutierrez*, Case No. 17 CV 2086 (S. D. Cal. 2017).

23 Complaint, *Securities & Exchange Commission v. Desarrolladora Homex S.A.B. DE C.V.*, Case No. 17 CV 432 (S. D. Cal. 2017).

24 Id.

25 SEC press release, 'SEC Charges Mexico-Based Homebuilder in $3.3 Billion Accounting Fraud' (3 March 2017) <https://www.sec.gov/news/pressrelease/2017-60.html>.

26 Matt Egan, 'Mexican company faked the building of 100,000 homes: SEC', *CNN Business* (3 March 2017) <https://money.cnn.com/2017/03/03/investing/mexico-homex-fraud-fake-home-sales/index.html>.

27 SEC press release, 'SEC Charges Mexico-Based Homebuilder in $3.3 Billion Accounting Fraud' (3 March 2017) <https://www.sec.gov/news/pressrelease/2017-60.html>.

Mexican government announced that it carried out the investigation jointly with the SEC and imposed its own penalties against Homex and some of its officials in addition to the penalties imposed by the SEC.[28] Mexico's National Banking and Securities Commission fined the company US$1.2 million.[29]

Mexico's enhanced corruption enforcement

During the past year, Mexico has made a concerted effort to enforce its existing criminal code to combat corruption. President López Obrador, who was elected in 2018, ran on a campaign of taking on the 'mafias of power' and shifting away from what has traditionally been viewed as relatively lax enforcement of Mexico's corruption laws.[30] Following López Obrador's election, the Senate enacted a new law that created a Chief Prosecutorial Office and appointed Alejandro Gertz Manero, a former attorney general of Mexico, to fill the role of chief prosecutor.[31] Gertz Manero announced in May 2019 that his office would begin building criminal corruption cases that had sat dormant in the previous administration.[32] At the time of López Obrador's election, more than 300,000 investigations – a disproportionate number of which related to bribery and corruption of elected officials – had been backlogged.[33]

Thus far, both López Obrador and Gertz Manero have made progress. In June 2019, the López Obrador administration froze assets and issued arrest warrants in connection with the sale of a fertiliser plant from a state-owned Mexican oil and gas company (Pemex) to one of Mexico's biggest multinational companies (AHMSA).[34] Efforts like these may well expand as further progress is made. Additionally, 18 anti-corruption magistrates are to be appointed to the Federal Tribunal for Administrative Justice, which has exclusive jurisdiction over grave administrative offences such as embezzlement and money laundering.[35] Further implementation of Mexico's National Anti-Corruption System – a framework for a tougher and more comprehensive approach to battling corruption – is also planned.[36]

28 Sanctions to the Homex issuer, Government of Mexico <https://www.gob.mx/cnbv/prensa/sanciones-a-la-emisora-homex?idiom=es>.

29 Richard Marosi, 'Mexico's Homex faces accusations of massive fraud from the SEC, but the case has stalled', *Los Angeles Times* (2 March 2018) <https://www.latimes.com/world/mexico-americas/la-me-homex-sec-20180302-story.html>.

30 Martha Mallory, 'Mexico joins the anti-bribery enforcement bandwagon', *The FCPA Blog* (12 June 2019) <https://www.fcpablog.com/blog/2019/6/13/mexico-joins-the-anti-bribery-enforcement-bandwagon.html>.

31 Luis Dantón Martínez Corres, 'Mexico enforcement agencies eye "low hanging fruit"', *The FCPA Blog* (5 March 2019) <https://www.fcpablog.com/blog/2019/3/5/mexico-enforcement-agencies-eye-low-hanging-fruit.html>.

32 Brandt Leibe et al., H1 2019 Latin American Enforcement Observations, King & Spalding (8 August 2019) <https://www.kslaw.com/blog-posts/h1-2019-latin-america-enforcement-observations-2>.

33 '300,000 incomplete investigations, anarchy and extravagant spending in AGO', *Mexico News Daily* (7 May 2019) <https://mexiconewsdaily.com/news/300000-incomplete-investigations/>.

34 Martha Mallory, 'Mexico joins the anti-bribery enforcement bandwagon' – see footnote 30.

35 Gina Hinojosa and Maureen Meyer, WOLA Report: The Future of Mexico's National Anti-Corruption System (7 August 2019) <https://www.wola.org/analysis/report-anticorruption-lopez-obrador-mexico/>.

36 Id.

Expansion of Mexico's anti-corruption laws

In August 2019, the Mexican government passed the National Law for Dominion Extinction, which will allow the federal government to transfer ownership of any type of property derived, or presumptively derived, from illegal activities without indemnity or payment to the owner.[37] The country simultaneously expanded the definition of the type of conduct that could trigger asset forfeiture to include corruption, both by corporate entities and public servants as private persons.[38]

In December 2018, the federal-level Citizen Participation Committee presented a proposal for a National Anti-Corruption Policy, with 60 priority strategies for combating corruption through investigations, awareness, civil involvement and access to public service.[39] The Committee has also advocated for whistleblower protections and greater autonomy for institutions involved in identifying official misconduct.[40]

With the renewed energy and focus on anti-corruption enforcement in Mexico, it is likely that corporations operating in Mexico will begin to face greater scrutiny from Mexican officials. If the current trajectory holds, corporations should expect Mexico to join the United States and Canada as a significant player in corporate anti-corruption efforts.

Co-operation between the United States and Canada

Recent cross-border interactions

Extradition of Meng Wanzhou

A matter that is currently unfolding – the arrest by Canadian authorities of a prominent Chinese national at the behest of the United States – has garnered widespread media attention. Meng Wanzhou, the chief financial officer, deputy chairwoman of the board of Chinese multinational technology company Huawei and daughter of Huawei's chief executive officer and founder, was arrested on 1 December 2018, at Vancouver International Airport, at the request of the DOJ on multiple federal criminal charges, such as bank fraud, trade secrets theft and sanctions evasion.[41] Meng is currently awaiting a hearing, scheduled for January 2020, on her possible extradition from Canada to the United States.[42]

Meng and her attorneys have vigorously disputed the charges, and called her arrest politically motivated. Lawyers for Meng also announced that they were suing the Royal Canadian Mounted Police (RCMP), the Canadian Border Services Agency and the Canadian federal

37 Carlos Leo Varelas, 'Compliance Alert: Mexican government grants itself right to seize and sell "unexplained" corporate assets', *The FCPA Blog* (16 August 2019) <https://www.fcpablog.com/blog/2019/8/16/compliance-alert-mexican-government-grants-itself-right-to-s.html>.

38 Luis Dantón Martínez and Juan José Paullada, 'Practice Alert: Mexico expands asset forfeiture to anti-corruption enforcement', *The FCPA Blog* (16 July 2019) <https://www.fcpablog.com/blog/2019/7/16/practice-alert-mexico-expands-asset-forfeiture-to-anti-corru.html>.

39 Gina Hinojosa and Maureen Meyer, WOLA Report – see footnote 35.

40 Andrew Levine, et al., 'Anti-Corruption Enforcement in Mexico: A Possible Turning Point?', Program on Corporate Compliance and Enforcement at New York University School of Law <https://wp.nyu.edu/compliance_enforcement/2019/08/12/anti-corruption-enforcement-in-mexico-a-possible-turning-point/>.

41 Julia Horowitz, 'Huawei CFO Meng Wanzhou arrested in Canada, faces extradition to United States', *CNN Business* (6 December 2018) <https://www.cnn.com/2018/12/05/tech/huawei-cfo-arrested-canada/index.html>.

42 Jill Disis, 'Huawei executive Meng Wanzhou claims US and Canada unlawfully detained her', *CNN Business* (21 August 2019) <https://www.cnn.com/2019/08/21/business/huawei-meng-wanzhou-extradition/index.html>.

government for breaching Meng's constitutional rights during her detention but prior to her arrest.[43]

Canada has faced significant backlash from China as a result of Meng's arrest, including the detention of Michael Kovrig, a former Canadian diplomat, and Michael Spavor, a Canadian businessman, under suspicions of spying and stealing state secrets; Canadian shipments to China of goods worth billions of dollars have also been blocked.[44] In addition, following the arrest of Meng, China quickly retried two Canadian citizens, who had been sentenced to jail for drugs smuggling, and sentenced both to death.

Kinross gold FCPA enforcement action

Co-operation between the United States and Canada on anti-corruption matters also continues. In March 2018, for example, the SEC announced a settled action against the Canadian corporation Kinross Gold Corporation for US Foreign Corrupt Practices Act (FCPA) books and records, and internal controls violations 'arising from the company's repeated failure to implement adequate accounting controls of two African subsidiaries'.[45] Kinross Gold had acquired a number of African subsidiaries in 2010 as part of a US$7.1 billion transaction and, according to the SEC, understood at the time that those subsidiaries 'lacked anti-corruption compliance programs and internal accounting controls'. The SEC alleged that, despite this awareness, Kinross Gold failed to implement adequate controls for more than three years, even though multiple internal audits had alerted the company to the control deficiencies.[46] Moreover, the SEC alleged that even after Kinross Gold implemented various internal controls, it failed to maintain them.[47] Without admitting or denying the findings, Kinross agreed to a cease-and-desist order, a penalty of US$950,000 and undertakings to report on its remedial steps for a period of one year.[48] Kinross Gold stated that it received a declination from the DOJ.[49]

Conviction of Robert Barra under the Corruption of Foreign Practices Act

Canada has recently enhanced enforcement of its own evolving anti-corruption laws. Prosecutions based on Canada's Corruption of Foreign Public Officials Act (CFPOA), the equivalent of the US FCPA, had been rare until recently. In 1998, 2004 and 2011, Canada was criticised by the Organization for Economic Co-operation and Development (OECD)

43 Dan Bilefsky, 'Meng Wanzhou's Cushy Bail Is Raising Hackles in Canada', *The New York Times* (4 March 2019) <https://www.nytimes.com/2019/03/04/world/canada/huawei-canada-meng-wanzhou.html>.

44 'Meng Wanzhou: Huawei CFO seeks halt to extradition after Trump comments', *The Guardian* (8 May 2019), <https://www.theguardian.com/technology/2019/may/09/meng-wanzhou-huawei-cfo-seeks-halt-to-extradition-after-trump-comments>.

45 SEC press release, 'Kinross Gold Charged With FCPA Violations' (26 March 2018) <https://www.sec.gov/news/press-release/2018-47>.

46 Id.

47 Id.

48 Id.

49 Richard L Cassin, 'Canadian gold miner resolves FCPA charges', *The FCPA Blog* (26 March 2018) <https://www.fcpablog.com/blog/2018/3/26/canadian-gold-miner-resolves-fcpa-charges.html.

for not meeting its OECD anti-corruption obligations.[50] In 2013, the CFPOA was amended to add a books and records offence, expand jurisdiction based on nationality, and increase the maximum penalty for convicted individuals.[51]

In January 2019, however, following only the second trial under the CFPOA, Robert Barra, a US citizen, was convicted in the Ontario Superior Court of Justice of agreeing to bribe a foreign public official.[52] The convictions in *R v. Barra and Govindia* arose from the same facts as a 2014 case, *R v. Karigar*, the first case in which an individual – Nazir Karigar, a Canadian – was sentenced to imprisonment for an offence under the CFPOA (he received three years in jail).[53] Barra, a former executive of the biometrics company Cryptometrics US, was charged in a conspiracy involving bribing various Air India employees, and a number of Indian government officials, to ensure that Cryptometrics was awarded a contract with Air India to instal facial recognition software at airports.[54] The complaint alleged that Barra 'was a co-Chief Executive Officer of Cryptometrics US, which he controlled' and that 'Cryptometrics US provided the required funding for Cryptometrics Canada's operations'.[55]

Shailesh Govindia, an Indian citizen, was also convicted. Govindia argued that he was not subject to the jurisdiction of the Canadian courts because, at the time of his conduct, he was unaware that the Canadian laws would apply to him. The court rejected this argument, finding 'that a Canadian court did have jurisdiction and that there was a substantial connection to Canada' and that Govindia's mistake of law was not a valid argument.[56]

That Canada used the CFPOA to charge a US citizen who was the executive of a US company for offences that occurred at least in part in New York may represent the beginning of a new era for Canadian enforcement of its bribery laws. The DOJ had long been aware of the allegations regarding Cryptometrics – as early as 2007, 'someone called Buddy sent an email to the fraud section of the US DOJ advising that he had information about US citizens paying bribes to foreign officers'.[57] The DOJ assisted the RCMP in the investigative efforts that led to Govindia's conviction in Canada.[58]

50 Global Affairs Canada, 'Bribery and corruption' <https://www.international.gc.ca/trade-agreements-accords-commerciaux/topics-domaines/other-autre/corruption.aspx?lang=eng>.

51 Id.

52 Lawrence E Ritchie, et al., 'Canadian prosecutors secure two more convictions in foreign corruption case', *Osler* (24 April 2019) <https://www.osler.com/en/blogs/risk/april-2019/canadian-prosecutors-secure-two-more-convictions-in-foreign-corruption-cas>.

53 '*R. v. Barra*: A timely but qualified success for Canada's corruption of foreign public officials regime', Dentons (8 March 2019) <https://www.dentons.com/en/insights/articles/2019/march/8/r-v-barra-a-timely-but-qualified-success-for-canadas-corruption-of-foreign-public-officials-regime>.

54 *R v. Barra and Govindia*, 2018 ONSC 57.

55 Id.

56 Govindia was aware, throughout the negotiations, that his meeting was with a Canadian company. *R v. Barra and Govindi*a, 2018 ONSC 57.

57 Id.

58 John Bray, 'Paying Bribes: How Not to Win Business', *Forbes* (27 February 2014) <https://www.forbes.com/sites/riskmap/2014/02/27/paying-bribes-how-not-to-win-business/#614f70157e04>.

Trends in cross-border investigations

Corporate frauds

On 19 September 2018, Canada's Criminal Code was amended to establish a Remediation Agreement (the equivalent of a deferred prosecution agreement in the United States), which may signal an increased focus on enforcement of the CFPOA with regard to corporations. This new tool will allow voluntary agreements between prosecutors and organisations accused of committing crimes, which the Canadian government hopes will provide an incentive for companies to rectify their wrongdoing, while avoiding some of the negative consequences of a criminal conviction.[59] Canada's Global Affairs department has described the new tool as 'available for use by prosecutorial authorities – at their discretion, in the public interest and in appropriate circumstances'.[60] Accordingly, Canada's new Remediation Agreement may allow the country to resolve its investigation regarding embattled engineering giant, SNC-Lavalin, which has been involved in an ongoing foreign bribery investigation.[61]

Competition protection enforcement in the digital economy

The co-operation between the United States and Canada is not limited to criminal actions and securities enforcement. US–Canadian co-operation with regard to antitrust and consumer protection matters has evolved into a robust bilateral enforcement regime. Following the August 1995 Agreement between the Government of Canada and the Government of the United States of America Regarding the Application of Their Competition and Deceptive Marketing Practices Laws (the Agreement), the two nations have closely coordinated on common consumer protection matters.[62] The Agreement sets forth seven obligations for each nation:

- notification about enforcement activities in the other's interests;
- co-operation in enforcement and information exchange;
- coordination in enforcement initiatives;
- avoidance of conflicts;
- consultations to resolve concerns regarding the agreement;
- maintenance of confidentiality; and
- use of principles of comity.[63]

59 Government of Canada, Remediation Agreements and Orders to Address Corporate Crime <https://www.canada.ca/en/department-justice/news/2018/03/remediation-agreements-to-address-corporate-crime.html>.

60 Global Affairs Canada, 'Bribery and corruption' – see footnote 50.

61 See, e.g., Joanna Harrington, 'SNC-Lavalin case shows why we should review Canada's foreign corruption laws', *National Post* (27 February 2019) <https://nationalpost.com/pmn/news-pmn/snc-lavalin-case-shows-why-we-should-review-canadas-foreign-corruption-laws>.

62 Government of Canada, Agreement between the Government of Canada and the Government of the United States of America on the application of positive comity principles to the enforcement of their competition laws <https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/01269.html>.

63 Debra A Valentine, 'Cross-Border Canada/U.S. Cooperation in Investigations and Enforcement Actions', US Federal Trade Commission (15 April 2000) <https://www.ftc.gov/public-statements/2000/04/cross-border-canadaus-cooperation-investigations-and-enforcement-actions>.

Though these obligations had been in effect for more than 20 years, in 2017 both countries recommitted to strengthening North American co-operation in competition law enforcement in the digital economy.[64] Since this agreement, both countries have made strides towards improving antitrust enforcement in the digital space. Canada unveiled a new Digital Charter, designed to maintain a competitive online marketplace, increased fines and penalties to encourage global digital leaders to promote compliance, increased global enforcement coordination, and hosted a global summit to discuss competition policy in the digital era.[65]

The US Federal Trade Commission likewise recently launched a Technology Task Force, which is dedicated to monitoring competition in US technology markets, and Congressional leaders have taken an interest in understanding competition in the digital marketplace.[66]

Given these trends, and the standing Agreement between the United States and Canada, it is likely that corporations will see increased co-operation between the two countries on digital antitrust enforcement in the coming years.

64 Government of Canada, 'Competition Bureau reinforces ties with U.S. and Mexican competition authorities' (20 November 2017) <https://www.canada.ca/en/competition-bureau/news/2017/11/competition_bureaureinforcestieswithusandmexicancompetitionautho.htm>.

65 Dominic Thérien, et al., 'The New Commissioner of Competition Requests Changes to Address Digital Economy Challenges', *Mondaq* (4 June 2019) <http://www.mondaq.com/canada/x/816628/Data+Protection+Privacy/The+New+Commissioner+Of+Competition+Requests+Changes+To+Address+Digital+Economy+Challenges>.

66 Peter J Levitas, et al., 'Antitrust Scrutiny of High-Tech: What Does it Really Mean?', Arnold & Porter (15 August 2019) <https://www.arnoldporter.com/en/perspectives/publications/2019/08/antitrust-scrutiny-of-hightech>.

Part II

Investigations Country by Country

5

Argentina

Pedro Serrano Espelta, Gustavo Morales Oliver and María Lorena Schiariti[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The *Notebooks* case is the highest-profile ongoing investigation for bribery-related crimes, at the time of writing. The investigation was initiated in early 2018 and involves various high-ranking current or former public officials and numerous businessmen.

The case is moving on to trial. It has triggered other parallel investigations, such as the investigation of the Antitrust Commission for cartelisation.

2 Outline the legal framework for corporate liability in your country.

Currently there are several statutes that establish criminal sanctions for corporations in Argentina. The most notable is the Law No. 27,401 (on corporate criminal liability), which entered into force on March 2018. Corporations can also incur liability for economic crimes as prescribed in section XIII of the Federal Criminal Code, or by virtue of a breach of any of the following statutes:

- Customs Code Law No. 22,415;
- Foreign Exchange Criminal Law No. 19,359;
- Tax Criminal Law No. 27,430;
- Competition Law No. 27,442;
- Supply Law No. 20,680; and
- Retirement and Pension System Law No. 24,241.

1 Pedro Serrano Espelta, Gustavo Morales Oliver and María Lorena Schiariti are partners at Marval, O'Farrell & Mairal.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Corporations are regulated by the relevant public register of commerce as well as other government agencies, for example, the Argentine tax authority (AFIP).

Also, depending on the industry, additional regulatory agencies or entities may issue regulations that govern corporations' activities, such as the Argentine Securities Commission for corporations that trade securities, or the Argentine Central Bank for corporations that provide certain financial services or products.

Jurisdiction between the authorities based on their subject matter and competence is allocated by territory.

There are no specific policies or protocols relating to the prosecution of corporations.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

In some instances, the law indicates the degree of suspicion to initiate or defer an investigation to another agency. The Anti-money Laundering Law No. 25,246 establishes that the Argentine Financial Intelligence Unit shall notify the public prosecutor when there are 'sufficient elements of conviction' to determine that an operation under review may indicate a case of money laundering or terrorism financing.

As regards criminal investigation, the mere affirmation of the possible existence of a crime is enough to start an investigation. The authorities have the duty to investigate all facts that come to their knowledge and can constitute a crime under their jurisdiction.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A notice or subpoena may be challenged through a procedural remedy requesting it to be declared null. It may be admissible when the notice or subpoena contains a serious irregularity that prevents the party from promptly complying with the obligations that stem from it.

The most common irregularities that give grounds for challenging a notice or subpoena include that the notice does not contain the court details, the court details are wrong, or service of the complaint was effected in a domicile other than that of the defendant.

If the notice or subpoena is issued by an administrative authority, it must first be challenged before the administrative authority to allow questioning before the courts.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Argentine law allows individuals suspected of participating in certain crimes set forth in Law No. 27,304 to enter into collaboration agreements with the prosecution. Under this regime, suspects and defendants who provide relevant information may obtain a penalty reduction in exchange of their assistance. Once signed, the collaboration agreement has to be submitted to the court for approval.

As regards legal entities, Law No. 27,401, for example, includes the possibility for corporations under investigation to sign collaboration agreements with the prosecution. The corporation must provide useful and verifiable information or accurate details that assist in clarifying the facts under investigation, identify the persons involved, or recover the assets or proceeds of the crime, among other requirements. Once signed, the collaboration agreement has to be submitted to the court for approval.

7 What are the top priorities for your country's law enforcement authorities?

The Office of the Federal Public Prosecutor has not issued policy papers stating its current priorities. However, recently there has been a reported interest in economic and financial crimes, such as money laundering, as well as public bribery and corruption offences.

Also relevant are drug crimes and gender-based violence.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Argentina lacks a comprehensive legal framework addressing cybersecurity issues. However, there are certain resolutions ruling cybersecurity issues applicable to the public sector. Technological Standards for the Federal Public Administration were approved by Disposition 5/2019, published in the Official Gazette on 2 September 2019.

The Argentine Data Protection Authority (ADPA) has issued Resolution No. 47/2018, which establishes two sets of recommended security measures for the processing and conservation of personal data with the aim of ensuring the continuous improvement of the administration, planning and control of information security.

Resolution 47/2018 entails a change in the approach towards personal data security that follows the principle of accountability, introduced by ADPA in other recent regulations and in line with the European General Data Protection Regulation. It is worth noting that among these recommended measures, Resolution 47/2018 lists that security incidents should be notified to ADPA.

Certain industries have their own cybersecurity regulations and standards (e.g., financial institutions are required to report security incidents to the Argentine Central Bank).

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

On 22 November 2017, the Argentine Congress signed the Convention on Cybercrime of the Council of Europe (ETS No. 185) adopted in Budapest, Hungary, on 23 November 2001 (the Budapest Convention), but is still pending enactment by the president.

In 2008, Argentina passed the Cybercrime Law No. 26,338 and amended its Criminal Code to include several cybercrimes, modelling them on those contained in the Budapest Convention. Consequently, the new aspects relate to procedural law and international co-operation. Argentina still uses these rules for securing physical evidence for searches in computer systems, which is inefficient from a digital evidence standpoint.

Regarding the approach by law enforcement authorities, various federal and local authorities (including prosecutors and police) have created specialist cybercrime units.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Overall, Argentine criminal law is applicable to acts committed in its territory and places under its jurisdiction (e.g., national aircraft and embassies).

The application of local criminal law will be extended to acts committed abroad the effects of which are deemed to be produced in the territory of Argentina or places under its jurisdiction.

Likewise, Argentine criminal law will apply to offences committed abroad by federal authorities' agents or employees in the exercise of their public functions. Moreover, criminal law will apply to bribery of foreign officials committed abroad by Argentine citizens and legal entities domiciled in Argentina.

Finally, Argentina has ratified several treaties that establish universal jurisdiction over serious crimes, such as genocide and torture.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

There are many legal, operative, strategic, technological, communicational and accounting challenges in cross-border investigations that arise in the initial stage and continue throughout the investigatory process. The most important challenges are the protection of the attorney–client privilege and compliance with data privacy and data protection regulation, especially across jurisdictions that have different legal standards of compliance.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Argentine law protects against double jeopardy, that is to say a person who has been convicted or acquitted of an offence cannot be prosecuted again for the same offence.

The principle of double jeopardy (also known as *ne bis in idem*) is established in the Federal Criminal Code, the Federal Constitution and certain human rights treaties that have constitutional hierarchy in Argentina. The law does not distinguish between federal and foreign jurisdictions when it prohibits double jeopardy. Depending on the jurisdictions involved, there may be co-operation treaties establishing rules to resolve a potential double jeopardy conflict.

The fact that a corporation has entered into a deferred prosecution agreement (DPA) in another country is unlikely to prevent prosecution in Argentina, unless a treaty prescribes

otherwise or the DPA is viewed as being equivalent to an acquittal, a conviction or any other decision that puts an end to the criminal proceeding.

There is nothing analogous to the United States 'anti-piling on' policy between Argentinian law enforcement authorities.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not usual in cases investigated by Argentinian authorities.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Decisions made by foreign authorities may attract the attention of Argentine authorities and be the catalyst for local investigations.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Argentina has not implemented a specific autonomous trade sanctions system. However, Argentina complies with the sanctions established in the United Nations Security Council's resolutions. In that context, compliance with the sanctions established therein is mandatory for Argentina. Also, once the Ministry of Foreign Affairs publishes the United Nations Security Council's resolutions in the Argentine Official Gazette, those sanctions regimes become mandatory for Argentine individuals and legal entities.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Argentina has not conducted any relevant enforcement activity.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Argentina has not conducted any relevant enforcement activity.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Law No. 24,871 regulates the extent of the application of foreign regulations. In particular, it sets forth that any foreign laws establishing extraterritorial sanctions intended to trigger, for example, negative consequences on a third country, would be deemed null and inapplicable in Argentina.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Any individual or legal entity shall not invoke rights, execute or claim the execution of acts nor be compelled to comply with measures, orders, instructions or indications that are a consequence of the extraterritorial application of foreign regulations, as referred to in question 18.

Additionally, Law No. 24,871 establishes additional provisions regarding, for example, the enforcement of foreign rulings under the aforementioned foreign regulations, or the exchange of information between Argentine authorities and the authorities of the foreign country issuing sanctions.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

In our experience, most allegations of wrongdoing in companies in Argentina have been made through whistleblower reports on ethical lines.

In our experience, in many cases, when an issue comes to light as a result of a regular internal auditing process, most companies fail to take early action to investigate the matter.

Information gathering

21 Does your country have a data protection regime?

Personal data protection is governed by Personal Data Protection Law No. 25,326 (PDPL), which has the main purposes of guaranteeing (1) the complete protection of the data contained in files, records, databases or other technical means, whether public or private, and (2) the rights to reputation, privacy and access to information. Any information relating to individuals or companies, whether identified or identifiable, is considered personal data and subject to the terms of the PDPL.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The PDPL is enforced by ADPA and the judicial courts. Depending on the type of behaviour, failure to comply with the PDPL could be considered as minor, serious or very serious infractions.

During 2018, ADPA imposed sanctions with fines for an accumulated amount of 71,625,320 Argentine pesos.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

As a general rule, valid data treatment requires the free, express, informed and written (or similar) consent of the data subject (i.e., the relevant individual or legal entity). Data subjects are free to revoke their consent, although this will only have effect for the future (not retrospectively). They also have the right to have access to, rectify and delete their personal data.

Treatment of data that is limited to the data subject's name, identification number, tax identification number, occupation, date of birth and domicile, does not require consent.

Moreover, the PDPL determines restrictions to cross-border transfers of data.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

From a privacy perspective, it is highly important to provide employees with prior notice explaining the way in which the company treats the data they use (generally through corporate IT or privacy policies).

From a labour law perspective, there are no specific regulations in force regarding the access, monitoring and surveillance of electronic communications and devices in the workplace.

It is of key importance to analyse any internal policy (duly notified to the employees) relating to the monitoring of corporate emails and, upon default thereof, implement an internal policy for the monitoring of emails, electronic communications and devices, and the use of working tools and to notify employees in advance that (1) electronic communications and devices are work tools and, thus, they shall be used only for work purposes and (2) they should have no expectation of privacy in connection with their use (even if a personal password has been created). Further, a company should have in place further provisions for monitoring employees' activity and ultimately to prove misconduct.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

According to the Federal Criminal Procedural Code, if there is reason to presume that in a certain place there are things relating to the investigation of a crime, or the suspicion of a criminal offence, a judge may issue a search warrant. Further, a judge may order the seizure of objects and documentation that (1) may be relevant to the investigation, (2) may be subject to confiscation or (3) can serve as evidence.

Besides the formal requirements, search warrants must indicate the crime under investigation, the exact place where the search will be conducted and its purpose. If any of these requirements are not fulfilled, the search – and any evidence collected during the search – can be challenged in court.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

The Federal Criminal Procedural Code protects letters and documents sent to or received by a defendant's counsel from being seized, as long as they are connected to a criminal investigation.

Moreover, a judge may request the testimony of witnesses and third parties and the submission of documents in their possession. However, this order shall not be addressed to persons exempted from testifying as witnesses by reason of family or professional links, or state secrecy.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Judges can request the testimony of any person who may have relevant information relating to a criminal investigation. The request is mandatory and the person summoned to render testimony must appear before the judge and state the truth of what they know, unless an exception applies. Failure to do so may be construed as contempt of court or harbouring, and may trigger raids to seize the information. According to Argentine law, these offences are only attributable to individuals.

Argentine law protects the right against self-incrimination. For instance, when a representative of a legal entity is called to give information relating to a criminal investigation, the representative may refuse to give testimony on the basis of the constitutional right against self-incrimination.

Additionally, the Federal Criminal Procedural Code establishes that those who must keep the secrecy of what they learn by virtue of their service, profession or official capacity must abstain from rendering testimony of facts and issues covered by such secrecy. Among the persons expressly included are lawyers, notaries, doctors, nurses, military personnel and public officials. However, they cannot refuse to give testimony when released from their secrecy duty by the interested party, for instance.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Law No. 27,319 regulates special investigation techniques than can be used in the investigation of certain complex crimes, such as drug-related crimes, smuggling, terrorism and economic crimes.

Under this framework, persons who provide useful and relevant information to initiate or guide an investigation concerning the crimes set forth in the law will be entitled to receive monetary compensation. The identity of whistleblowers will be withheld and, if necessary, other adequate protective measures may be ordered to protect the life and integrity of the whistleblower and his or her family.

Depending on the circumstances, other regimes may apply. For instance, recently a permanent rewards fund for whistleblowers created in 2009 was used to offer monetary rewards in exchange for useful information to trace and recover assets in a high-profile corruption case.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

There is no specific labour regulation concerning investigations or a specific procedure for internal investigations. Nevertheless, labour and civil rights are fully applicable to all employees. Thus, it is important to bear in mind that any kind of discrimination or adverse

effect on employees' dignity or right of defence could be challenged within the context of the investigation.

Investigations should be carried out as quickly as possible, so that disciplinary action, if any, can be decided as soon as possible after discovery of the behaviour under investigation.

If the personnel involved are board members or authorised signatories of the company, measures regarding removal of control and replacement to ensure the normal operation of the company should be jointly analysed.

Additionally, since each case will be different on its merits, there could be different practical matters to consider within the context of a labour investigation; thus, it is important to duly liaise with the appropriate legal adviser.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Different courses of action and different sanctions could be implemented, depending on the seriousness of the misconduct, the extent to which it affects the employer's activity or business, the level of responsibility of the relevant employee, previous performance, among other aspects, all of which should be considered in each case.

Damage caused by the misconduct could also be considered, although this is not essential since the misconduct itself could be subject to disciplinary measures. Possible sanctions could involve a first warning, suspension from duty without payment of salary or even dismissal with just cause, subject to full analysis of the case in question.

Prior to implementing any course of action or disciplinary sanction, it is important to bear in mind that (1) there are both specific requirements applicable to disciplinary sanctions and practical legal recommendations, and (2) dismissal with just cause is interpreted narrowly in Argentina.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

Employees are entitled to refuse to participate in an internal investigation, without their refusal construing a just cause for termination of the employment contract.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Before commencing an internal investigation, it is useful for companies to draft a flexible investigation plan, which may lead the investigation process and determine, among other things, its scope, time limits and main objectives.

There is currently no legal requirement regarding the need for an investigation plan. Therefore, in practice, implementing such a plan depends on each company, the complexity of the subject under investigation and the regulations involved.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Law No. 27,401 (on corporate criminal liability) addresses the concept of internal investigations and sets forth that each legal entity, depending on the risks to its activities, may implement an internal investigation system.

In general, there is no particular legal obligation to comply with when misconduct comes to light in the course of an internal investigation; however, certain industry-specific regulations may establish additional provisions regarding internal investigations, which companies should take into account.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

If a company receives a notice seeking the production of documentation or a subpoena requiring its testimony to clarify the facts or allegations under investigation, the company shall comply within the terms specified, unless it is subject to any exception provided in the applicable regulation.

There is no specific regulation setting forth mandatory steps for companies to comply with such notices or subpoenas. Therefore, the measures implemented may depend on the company's policies and procedures, the facts and persons under investigation, and so on.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

A public company in Argentina is not obliged to disclose the existence of an internal investigation until the investigation results in verification of the existence of an event that, in all likelihood, could have a substantial effect on its trading value (except when an investigation was commenced following verification of the existence of an event having such effects, which must be disclosed). Likewise, there is no obligation to disclose any contact by a law enforcement authority until the company is served with notice of the commencement of formal proceedings (except where such circumstances are made public or disclosure is required by a law enforcement authority).

36 How are internal investigations viewed by local enforcement bodies in your country?

Provided that the rights of employees are respected, internal investigations are well tolerated. Investigations of wrongdoings and crimes in Argentina are usually conducted by law enforcement authorities; therefore, as yet, acceptance among local agencies is not widespread.

Law No. 27,401 (on corporate criminal liability) encourages companies to implement an internal investigation system that respects the rights of the persons under investigation and permits the imposition of effective sanctions on those who breach the company's policies.

In this sense, an internal investigation may be useful to show to the authorities that the company acted diligently and in good faith to try to prevent, identify and remedy a potential wrongdoing. Given the recent enactment of Law No. 27,401 there are no precedents yet to establish how law enforcement agencies will assess the efforts taken by companies during an internal investigation.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Attorney–client privilege stems from the constitutional right to defence during trial. Criminal procedure codes prohibit disclosure of protected confidential information when obtained by certain professionals when performing as such, including attorneys and doctors. Further, the Federal Civil Procedure Code establishes that a witness may refuse to answer questions if the answers may disclose information protected by the attorney–client privilege.

There is very little legislation and jurisprudence regarding the attorney–client privilege on internal investigations. As a minimum, all attorney work-product is protected by the attorney–client privilege. Marking documents as confidential and protected by attorney–client privilege is recommended.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The Federal Supreme Court has ruled that privilege protects documents or communications held on the occasion or in the performance of the profession of attorney. Another key principle is that the client may waive the privilege.

The holder of the privilege is the client, and the attorney has the duty and the right to protect the privileged information.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

There are no legal standards in Argentina for this. However, according to the majority of legal experts, provided the attorney is a member of a professional association, the attorney–client privilege will apply if he or she is either in-house or external counsel.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

The applicable regulation in Argentina does not make any difference between advice sought from foreign and local lawyers. Privilege should apply equally to both.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

There are no precedents that would allow us to consider the waiver of attorney–client privilege as a co-operative step. Privilege waiver is not mandatory or required.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The applicable regulations do not stipulate partial waivers.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

There is no developed jurisprudence on this matter.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

This concept does not exist in Argentina.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

There are no material studies or case precedents in Argentina that would allow us to conclude that privilege protects the work-product of third parties that assisted the work performed by the lawyer.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Witness interviews as part of internal investigations are not forbidden or specifically regulated in Argentina.

Nonetheless, the Guidelines of the Argentine Anti-corruption Office on Compliance Anti-corruption Programmes briefly address certain mechanisms for corporate investigations, including witness interviews. In particular, the Guidelines emphasise that all the investigative mechanisms carried out by companies shall not put the employees' rights in jeopardy.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

There is no law that particularly regulates the extent of attorney–client privilege in internal investigations. In this context, a company may claim attorney–client privilege over internal witness interviews or attorney reports, but its chances of success will depend on the factors relevant to the case.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There is neither Argentine regulation nor relevant judicial precedents setting forth legal or ethical requirements or guidance for conducting witness interviews, whether they involve employee or third parties (e.g., former employees or contractors).

We advise our clients to apply internationally accepted common practices, such as providing *Upjohn* warnings to interviewees, avoiding recording interviews and preparing reports that merely include attorneys' impressions on the topics addressed in the interviews.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

The timing, order and steps taken in each interview (e.g., putting documents to the witness) will vary from case to case.

We advise our clients to consider all factors and good practices, as mentioned in question 48, when carrying out interviews. There are case precedents that acknowledge, for example, a witness's rights to be informed about the scope and nature of an interview, and to be accompanied at the interview by their own lawyer.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Under Argentine law, there is no general obligation to report misconduct to law enforcement authorities. However, depending on the industry, some laws and regulations may mandate companies to disclose certain forms of misconduct to the authorities.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting in Argentina is still unusual. Whether this is a convenient course of action will depend on the case in question.

Generally speaking, a company might be advised to self-report if it is likely to receive some leniency from the authorities. For instance, Law No. 27,401 (on corporate criminal liability) provides a regime under which companies may seek exemption from criminal liability. It also allows legal entities seeking a reduction in penalties to enter into 'effective collaboration agreements' with the authorities (see question 52).

The decision to self-report to foreign authorities should be made having taken into account the law of the jurisdictions involved and the particular facts of the case.

Note that public officials have a duty to report offences that are known to them in the exercise of their public functions. Directors of state-owned companies and those appointed by the government might be considered public officials for the purpose of this reporting duty.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

The particular steps to be taken will depend on the requirements imposed by the respective applicable laws and competent authorities.

For instance, Law No. 27,401 (on corporate criminal liability) provides a regime for companies to obtain an exemption from criminal liability and for it to be possible to sign 'effective collaboration agreements' with the prosecution to obtain a reduction in applicable penalties.

In the former situation, the law requires self-reporting of a crime as a consequence of internal detection and investigation, which suggests that conducting an internal investigation will be necessary to engage in negotiations with the prosecution.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

In the case of a judicial notice or subpoena, the company must respond to it through judicial channels within the relevant legal terms laid down under the Procedure Code.

It is possible to enter into dialogue with the authorities to establish the position of the defendants. However, official challenges, requests and decisions must be made through judicial or administrative channels, according to the relevant procedural rules.

54 Are ongoing authority investigations subject to challenge before the courts?

Any decision issued by the centralised or decentralised federal administration is deemed legitimate, but could be challenged before courts if the requisites set forth in the applicable administrative regulations of the proceedings are fulfilled.

Since Argentina is a federal country, depending on the territorial competence of the relevant authorities, local regulations may be applicable and the particular requisites established therein shall be taken into account.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

There is no general statute covering this matter. The approach will have to be assessed for each case, taking into account applicable laws and international treaties, if any.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

The company must comply with the requirement for production of material relating to a particular matter that crosses borders. However, according to the Federal Civil and

Commercial Procedural Code, it is necessary to establish whether the company in question is party to the proceedings or not.

In the case of companies acting as plaintiffs or defendants, they must produce the required material (documents or information) that is in their possession, even when the documents or information are outside the country.

If the company is a third party to the procedure in which the requirement is made, it is also obliged to produce the documents or provide the required information. However, the requested party may challenge the request if the material required is its exclusive property and its disclosure may cause damage.

The company that intends to produce material that is abroad will face certain difficulties that could delay the procedure. For instance, the company must comply with the requirements imposed by international treaties to verify the authenticity of foreign documents (i.e., through the Hague Apostille or authentication through diplomatic channels as well as translations, among other things). Further, the attendant costs could be significantly higher.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

The frequency of co-operation and challenges to co-operation vary according to the law enforcement authorities involved.

On the one hand, in respect of judges and prosecutors, cross-border co-operation and exchanges of information usually proceeds after a long period of time because of the many difficulties that can arise. For instance, in the *Operation Car Wash* bribery cases, leniency agreements and evidence produced in Brazil and requested by Argentine authorities are still pending.

On the other hand, certain law enforcement authorities frequently share information within the federal administration. For example, the Argentine Financial Intelligence Unit – being a member of the Egmont Group of Financial Intelligence Units – shares information with other units across the world, and the AFIP shares information in accordance with the Common Reporting Standard, among other methods.

Additionally, international treaties (either multinational or bilateral) may govern cross-border co-operation.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Overall, law enforcement authorities are bound to maintain confidentiality with respect to information obtained during investigations. They shall not share or disclose information or documents unless such conduct falls within one of the exceptions set forth in their statutes or applicable laws.

In some cases, the law allows the transfer of information between law enforcement agencies. For instance, the AFIP may share certain information with revenue agencies from the provinces, or foreign tax agencies, in accordance with applicable co-operation agreements.

In the course of a criminal investigation, the secrecy of the proceedings shall be respected. In particular, under Law No. 27,401, when corporations enter into negotiations with the prosecution with the aim of concluding a collaboration agreement, the information shared will be kept confidential.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

In these circumstances, companies should claim an exception and inform the relevant law enforcement authority that they cannot reasonably comply with the request without violating the laws of another country.

In addition, foreign legal advice should be obtained as to the company's exposure to liability if it produces the requested information.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Certain statutes and regulations set forth secrecy obligations, including those relating to banking (Law No. 21,526), tax (Law No. 11,683) certain professions (e.g., attorneys, health professionals) and confidential commercial information (Law No. 24,766). These statutes and certain regulations (e.g., Anti-money Laundering Law No. 25,246) establish certain circumstances when secrecy does not prevail and compliance with a notice or subpoena becomes mandatory.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

The rules applicable in a certain jurisdiction and the type of proceeding initiated against a company will determine the applicable rules of evidence. Nonetheless, Argentina does not regulate discovery rules. Thus, production is usually compelled by law enforcement authorities and interested parties can occasionally produce complementary evidence (e.g., expert witnesses).

Production of evidence within civil procedures is usually available to the parties and any other stakeholder, unless confidentiality is expressly imposed, which may be the case, for instance, in procedures where family issues are in question or when minors are involved.

Production of evidence within criminal procedures is confidential and withheld from the parties (including private prosecutors) during the investigative stage. However, during the trial stage, production of evidence is, in general, not subject to confidentiality and is accessible by the general public.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Companies may be subject to the following penalties:

- fines that normally will be determined based on the 'undue' benefit obtained or that could have been obtained through the crime;
- total or partial suspension of activities;
- debarment from participating in government bids and contracts, or in any other activity relating to the government;
- dissolution and liquidation of the legal entity;
- suspension or termination of government benefits;
- publication of the conviction sentence at the cost of the convicted entity; and
- forfeiture of assets obtained through the illegal actions.

Directors, officers and employees are subject to the penalties prescribed for the specific crime in the relevant statutes. Penalties for individuals include imprisonment, fines and debarment. Additionally, defendants may be subject to forfeiture of assets that have been obtained illegally.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Depending on the circumstances (such as the existence of a criminal investigation or whether precautionary measures were issued against the company), there might be restrictions on relocating assets sited or registered in Argentina to another country.

64 What do the authorities in your country take into account when fixing penalties?

In a criminal trial, judges must refer to the penalty scale of the crimes and take into account aggravating and mitigating circumstances, whenever applicable. Additionally, they will consider, among other things:

- the nature of the conduct;
- the means employed to commit the crime;
- the injury or risks caused;
- personal circumstances of the defendant, such as his or her age, education;
- conduct during the proceedings;
- motive to commit the crime (especially state of necessity or indigence);
- degree of participation in the crime; and
- recidivism.

Moreover, in respect of economic and financial crimes committed with intervention, on behalf, or for the benefit, of a legal entity, judges will also consider:

- compliance with internal rules and procedures;
- failure to monitor the conduct of the perpetrators and accomplices;
- the extent of the damage caused;

- the amounts of money involved;
- the size, nature and economic capacity of the legal entity; and
- the need to continue the activities of the company (for the purposes of suspension or debarment).

Finally, in respect of publicly traded companies, penalties shall be prescribed having in mind the protection of shareholders to whom no liability is attributable.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Since the enactment of the Law No. 27,401 (on corporate criminal liability), corporations can enter into agreements with the prosecution. The law envisions two sets of circumstances:

- It allows companies to be exempted from criminal liability when they have:
  - self-reported a crime set forth in that law as a consequence of internal detection and investigation;
  - established a proper control and supervision system before the facts under investigation occurred and breaching this system required an effort by the wrongdoers; and
  - returned the undue benefit obtained.
- Companies may execute 'effective collaboration agreements' with the prosecution to obtain a reduction of applicable penalties.

Companies must disclose precise and verifiable information that is useful for the investigation. The agreement is subject to court approval to enter into effect. At the time of writing, there are no precedents of collaboration agreements signed by corporations.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Argentina has regulated effective collaboration agreements in Law No. 27,401. Until the conclusion of an agreement with the public prosecutor, all negotiations are deemed to be strictly confidential.

The law makes no reference to the confidentiality of the information after the agreement is concluded and approved by the criminal judge. Therefore, there are no provisions that determine implementation of further restrictions or anonymity until the conclusion of the criminal proceedings. Consideration may be given to these measures in a particular case, depending on the potential risks that may affect a fair resolution of those proceedings.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

When considering entering into an agreement with any Argentine enforcement authority, a company should conduct a thorough analysis of the alleged facts and the possible legal

violations that may be triggered, either in Argentina or abroad. The company should also consider whether entering into a collaboration agreement would allow the authorities to gather information to prosecute other crimes.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Corporate compliance monitors are not regulated as an enforcement tool in Argentine law.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

When conduct gives rise to civil liability that also constitutes a crime, Argentine law allows both civil and criminal actions to be pursued simultaneously. Both proceedings are independent of each other; however, the civil judge is foreclosed from reaching a decision until a judgment is passed on the criminal case. Therefore, plaintiffs usually do not incur efforts and expenses until a decision is reached by the criminal court.

In criminal cases, the Federal Criminal Procedure Code recognises victims' right to offer and control evidence. It prescribes that the case docket is public to the parties, which includes the private prosecutor but not the civil petitioner, whose participation is limited to claiming compensation, restitution or other civil remedies. Despite this general principle, during the criminal investigation, judges may be reluctant to grant private prosecutors full access to some confidential information for reasons of security or privacy. During the trial, the private prosecutor has access to all files and evidence that will be used in court.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

In criminal investigations governed by the Federal Criminal Procedure Code, the docket file is withheld until the first appearance of the defendant before the judge (the investigative statement), where the defendant is put on notice about the investigation and informed of their rights.

However, third parties (e.g., the defendant, the victim and state authorities) may request information if they justify having a 'legitimate interest'. After this stage, the docket file can be accessed by the parties, including the defendant, the public prosecutor and the private prosecutor, if any. Notwithstanding, judges may order the secrecy of some information when disclosure would jeopardise the investigation. Only acts that cannot be reproduced at a subsequent stage shall not be kept confidential. The docket file will continue to be withheld from third parties during the investigation.

Once the case is in trial, hearings are public unless the court decides, as an exception, to restrain access by some or all public parties (e.g., relevant witnesses who have not yet given their testimony).

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

In our experience, companies have used both their in-house public communications department and external firms. Larger companies are more likely to retain the services of public relations companies when there is a risk of negative publicity.

72 How is publicity managed when there are ongoing related proceedings?

First, it should be assessed whether there are any disclosure restrictions. Public communications, whether involving an external public relations company or not, should be vetted by the company's legal adviser and the team in charge of litigation to ensure that there is nothing that could compromise the company's position in the proceedings.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Settlements are made within a criminal action, the existence of which must be disclosed upon service of process. Disclosure of settlements is forbidden until endorsement by the criminal court under penalty of sanctions under the Criminal Code.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Certain bills that address corporate misconduct, asset recovery and corruption-related crimes were recently introduced to the Argentine Congress. Additionally, a new bill to reform the Criminal Code was submitted to the Senate in March 2019. These bills are expected to be assessed in the near future.

Moreover, in view of the latest development in corporate governance matters, it is likely that regulatory bodies will issue specific regulations focusing on corporate misconduct and internal policies or procedures.

6

Australia

Ben Luscombe, Angela Pearsall, Tim Grave, Kirsten Scott and Lara Gotti[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

A Royal Commission into misconduct in the banking, superannuation and financial services industry (often described as The Banking Royal Commission or BRC) has received a high volume of media and industry attention, particularly since the release of its final report on 1 February 2019. As a result of the BRC's final report, the country's key corporate regulator, the Australian Securities and Investments Commission (ASIC) has publicly stated that it will adopt a 'why not litigate' enforcement approach, which will have a significant effect on its investigation and enforcement practices.

2 Outline the legal framework for corporate liability in your country.

Under Australian law, offences committed by 'a person' will, unless specifically excluded, include a corporation (including those offences punishable by imprisonment). Criminal liability is generally established if both a physical and fault element is proven. Fault elements include intention, knowledge, recklessness and negligence. In the case of strict or absolute liability offences, there are exceptions to the proof of fault elements. These offences are more commonly pursued against a corporation.

If a fault element is required to be proved against a corporation, it may be shown in a variety of statutorily defined ways, including by proof that a corporation failed to maintain a corporate culture of compliance.

1 Ben Luscombe, Angela Pearsall and Tim Grave are partners, Kirsten Scott is a counsel and Lara Gotti is a senior associate at Clifford Chance.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Regulation of Australian companies is principally done at a federal level, with some limited involvement by state or territory regulators. There is a broad range of law enforcement agencies that have authority to investigate corporations, including but not limited to the following:

- ASIC, an independent statutory body that enforces and administers the Corporations Act 2001 (Cth) (the Corporations Act), which is the main corporations legislation in Australia;
- Australian Prudential Regulatory Authority (APRA), a statutory body that supervises the banking, insurance and superannuation bodies;
- Australian Competition and Consumer Commission (ACCC), which regulates the interaction between consumers and businesses;
- Australian Criminal Intelligence Commission, which investigates national serious and organised crime, such as cybercrime;
- Australian Federal Police (AFP), which investigates and enforces cross-border compliance, including fraud, drug trafficking, organised crime, money laundering and people smuggling;
- Australian Taxation Office, which enforces compliance with Australia's taxation legislation;
- Australian Transaction Reports and Analysis Centre (AUSTRAC), which regulates and enforces cross-border financial transactions; and
- Commonwealth Director of Public Prosecutions (CDPP), which prosecutes criminal misconduct based on referrals from investigatory bodies.

Australian regulatory bodies coordinate their efforts so as to share information and intelligence-gathering powers (subject to certain restrictions). In the event of serious criminal allegations, it is common to have two or more regulatory authorities involved. Joint task forces, such as the Serious Financial Crime Taskforce, have been established to streamline and consolidate information sharing, investigation and reporting lines in Australia.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Regulators have wide-ranging statutory investigatory powers. The trigger point is generally suspicion of a breach of legislation within the regulator's jurisdiction. For example, an investigation under section 13 of the ASIC Act 2001 (Cth) will be triggered if ASIC thinks it expedient for the due administration of the corporations legislation and where it has reason to suspect that a contravention may have been committed. The degree of suspicion is not defined but the threshold is low.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A company should carefully consider the scope of the notice and any grounds for objecting to it, including whether it has been properly issued, the information sought is clearly defined and relevant, and the request is not oppressive or unreasonable. Any concerns should be

raised directly with the law enforcement authority before making an application to the court to set aside the notice.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Yes, in narrowly defined circumstances various enforcement bodies can apply their discretion for the benefit of defendants who assist with investigations. For example, the ACCC has a 'first past the post'-style policy that provides immunity to the individual or corporation who is first to disclose cartel conduct and co-operate fully with the investigation. The CDPP has a defined indemnity policy with strict criteria that must be met before a grant of immunity can be sought.

As to leniency, sentencing for criminal conduct is entirely at the discretion of the court. The High Court decision of *Barbaro* makes it clear that a prosecuting body cannot make submissions to the court regarding a preferred sentence or penalty range. More flexibility is provided for negotiated outcomes in civil penalty proceedings.

7 What are the top priorities for your country's law enforcement authorities?

Top priorities presently include misconduct in the financial services industry, financial crimes and corporate culture, including executive accountability. Cross-border business and transactions are also an area of focus, as are money laundering and tax evasion.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Cybersecurity is legislated at both a federal level, and a state and territory level through various legislative frameworks relating specifically to cybersecurity and more broadly to data protection and privacy. A Joint Cyber Security Centre has been established, which brings together business, government, academia and other key partners. In March 2019, the Australian government announced an intention to increase penalties under the Privacy Act 1988 (Cth) (the Privacy Act), from A$2.1 million to A$10 million, expand the regulator's scope to ensure breaches are addressed and add further protections to certain vulnerable groups.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Legislation provides regulation for computer and internet-related offences, such as unlawful access and computer trespass and creates investigation powers and criminal offences designed to protect security, reliability and integrity of computer data and electronic communication. There are also a number of offences addressing cybercrime contained in the Commonwealth Criminal Code.

Since March 2013, Australia has been a member of the Council of Europe Convention on Cybercrime, which addresses both domestic and international responses to cybercrime.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Criminal law has extraterritorial effect, provided there is an appropriate nexus to Australia. Conduct must have been either wholly or partly undertaken within Australia. Foreign entities with Australian subsidiaries or associated entities will fall within Australian laws as regards conduct in Australia. For example, if a foreign entity is conducting business in Australia through a subsidiary and the subsidiary breaches Australia's laws, both may be charged – the subsidiary for a breach of domestic laws and the foreign entity for directly breaching domestic laws or aiding and abetting the breach.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Australia has entered into mutual assistance treaties with numerous countries in a bid to facilitate information sharing and to expedite investigations. There are also information-sharing arrangements with certain jurisdictions, and therefore a formal request for mutual assistance is not always required. However, challenges arise when there are inconsistent approaches to an investigation by regulators. Legislative requirements as to the gathering of evidence, the integrity of investigators and the reliance on compulsory powers can present issues in cross-border matters.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

A person or corporation cannot be tried twice for the same alleged breach of Australian legislation. There is no prohibition in Australia against being prosecuted by multiple authorities where alleged contraventions of the law span the jurisdiction of multiple regulatory agencies; however, there is usually coordination between jurisdictions and agencies, to ensure prosecutions remain in the public interest.

However, double jeopardy does not apply internationally. Accordingly, if offending has traversed multiple jurisdictions, a defendant can be charged with an offence under Australian legislation despite having concluded proceedings of a similar nature in another country. A guilty plea or a negotiated outcome in another jurisdiction may affect the investigation, charge or sentencing in Australia.

There is nothing expressly analogous to the 'anti-piling on' policy in the United States.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not common, per se. Ordinarily, any negotiations regarding settlement in Australia will be influenced by settlements in other jurisdictions. ASIC's new 'why not litigate' approach may affect prospects for a 'global' settlement as ASIC will be keen to ensure any resolution withstands public comment in light of the BRC.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Given the co-operation mechanisms available to Australian regulators (such as mutual assistance agreements), it is possible to conduct concurrent investigations in multiple jurisdictions regarding the same factual matters. It is usual for one or more Australian investigatory bodies to coordinate domestically and with international investigatory bodies. A coordinated effort will usually result in one regulator taking the lead in an investigation and other jurisdictions supporting its efforts to round out the information gathering.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

The administration and implementation of Australia's sanctions laws is done at federal level, by the Department of Foreign Affairs and Trade (DFAT). Sanctions are implemented in accordance with the United Nations Security Council (UNSC) regime and further autonomous, Australian lead, sanctions regimes. DFAT has the power to issue a sanctions permit, should it be suitable, which will allow an importer or exporter to undertake activity that would otherwise contravene a sanction imposed in Australia. A full list of Australia's sanctions regimes is publicly available and it is expected that individuals and companies doing business in Australia should make their own enquiries to ensure compliance.

In April 2019, Australia imposed sanctions on the direct or indirect supply, sale or transfer to the Central African Republic on arms or related materials, without the issuance of a sanctions permit. In March 2019, Australia issued autonomous 'financial sanctions and travel bans on seven Russian individuals for their role in the interception and seizure of Ukrainian naval vessels'.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Australia is obliged to closely follow the UNSC in relation to enforcement of sanctions. Contraventions are enforceable against Australian individuals and companies, and certain sanctions will have effect irrespective of whether the activities are located in Australia or overseas. The Australian government has successfully prosecuted a number of companies for sanctions violations. A small number of individuals have also been charged.

In recent times, there has been discussion as to whether sanctions enforcement should also more readily incorporate AUSTRAC, which regulates cross-border monetary transactions, including money laundering and terrorism financing.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

DFAT may consult other Australian government agencies, other countries or the Sanctions Committee of the UNSC on a range of issues, including in consideration of whether to agree to a sanctions permit.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Australia currently does not have blocking legislation in relation to sanctions measures taken by third countries.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

There are a number of ways in which misconduct can be brought to the attention of a company, which include the following:

- ASIC conducts a preliminary investigation into every allegation of misconduct to assess whether further action is required. ASIC may be made aware of suspected contraventions by shareholders, media reports or whistleblowers.
- Whistleblower legislation requires that companies have avenues available to employees to report suspected misconduct. Whistleblowers may trigger internal investigations or investigations by ASIC.
- AUSTRAC monitors international transactions and transactions of (or more than) A$10,000 and will investigate any suspect transactions under anti-money laundering and counter-terrorism legislation.
- The Australian Securities Exchange (ASX) monitors share trading in publicly listed companies and can enquire into suspicious activities, including spikes in trading volume or share price. The ASX can refer suspected contraventions (such as insider trading) to ASIC for further investigation.

Information gathering

21 Does your country have a data protection regime?

The Privacy Act regulates the handling of personal information and the Australian Privacy Principles (APPs) provide guidelines for dealing with such information. The Notifiable Data Breaches scheme, established through the Privacy Act, obliges entities to notify individuals whose personal information is the subject of a data breach, and the Australian Information Commissioner, when it is likely the breach will result in serious harm.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The data protection regime is enforced through the Office of the Australian Information Commissioner (OAIC). The Privacy Act confers powers on the Commissioner to facilitate compliance with best practice. The OAIC's preferred regulatory approach is to facilitate compliance and prevent breaches although it also has investigative and enforcement powers.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

The APPs regulate how personal information is collected and used. If an entity investigates the actions of an employee, it must be careful that any personal data is collected in accordance with these principles. A heightened level of protection attaches to sensitive information, such as a person's religious beliefs, sexual orientation or health information. Entities must comply with their legal obligations, particularly those that require an employee to be notified that personal data has been collected. It is also important to consider any implications of cross-border transfer of personal information.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Employers are bound by contractual arrangements with employees, which often specify the rights an employer has over communications made during the course of employment. Interception of employment-based communications can be triggered by an internal investigation or well-founded suspicion of a contravention of company policy or legal obligations. Interception of personal, non-work-associated communications is governed by strictly applied privacy and telecommunications legislation and is likely to be illegal if beyond the scope of the employment arrangement. Enforcement of this legislation can involve the AFP.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Generally, the AFP executes search warrants on behalf of Commonwealth agencies. If an investigation is being conducted by another regulatory body, AFP officers may attend with

officers of that regulatory body. Warrants contain information as to the restrictions on entry time, dates and the evidence that can be gathered during the execution of the search warrant, which may include hard copies of documents as well as stored communications (such as computer hard drives or mobile phones). Defendants are entitled to have legal representatives present and to request an itemised list of the property seized, and have a right to challenge the warrant's validity.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Defendants may claim legal professional privilege (LPP) over materials seized during a legitimate search. Practically, this may mean the materials are sealed and delivered to the relevant court registry or regulator to await resolution of any disputed privilege claim by litigation or negotiation. The mere seizure of material without it being read does not constitute a waiver of privilege.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

During an investigation by a regulator, an individual can usually be compelled to give evidence in an examination. The individual cannot refuse to answer questions on the basis that those answers may tend to incriminate him or her. However, the individual can claim privilege against self-incrimination, meaning that the investigatory body cannot use the evidence gathered as an admission by the individual. There are some regulatory bodies that can derivatively use the information gathered during these types of examinations.

In a litigation context, an accused person has a right to claim privilege against self-incrimination or self-exposure to penalty, which means that they cannot be required to give evidence during proceedings against them. A witness may object to the giving of evidence in proceedings if the response would tend to prove that the witness had committed an offence under Australian or foreign laws or make them liable to a civil penalty.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Whistleblower legislation has undergone noteworthy amendment in 2019. Whistleblower protections apply to both current and former employees within a defined list of roles, reporting lines have been expanded and the role of a corporation in affording protections to whistleblowers has strengthened. It is a strict liability offence not to have a company policy relating to whistleblowing (companies are afforded some time since the implementation of the legislation to have this policy available).

There is no financial incentive programme in Australia for whistleblowers.

Corporate whistleblowers who provide information to ASIC about contraventions of the Corporations Act are granted three main legal protections, which are that:

- their identity and the information given cannot be disclosed unless authorised by law;
- they are protected against civil or criminal liability for making the disclosure (e.g., for defamation); and
- they are protected against being victimised for making their disclosure.

Protection will only be given to persons who meet certain criteria, including being an existing employee or officer of the company. In the financial sector, whistleblowers who provide information to APRA are given similar protections.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Under the Fair Work Act 2009 (Cth), certain employees are protected against unfair dismissal. In the event of an internal investigation, certain omissions by the employer may violate the right against unfair dismissal, including failing to provide the employee with a support person. The employee has a right to be given information relating to the allegations against him or her and adequate time to respond.

Under the Corporations Act, officers and directors are subject to significantly higher standards of conduct. Contravention of these duties may attract significant penalties, disqualification or imprisonment.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

If an employee has engaged in misconduct, his or her rights will depend on the precise nature of the misconduct. For example, an internal finding of serious misconduct may constitute valid grounds for dismissal. However, a finding of serious misconduct by law enforcement may constitute an offence, and the employee's rights would depend on the associated laws.

There are no express requirements for employers to impose disciplinary or other steps if an employee is suspected of misconduct.

If 'serious misconduct' is established, the employee's contract of employment may be immediately terminated. The Fair Work Regulations 2009 (Cth) define 'serious misconduct' as including wilful or deliberate behaviour that causes serious or imminent risk to the health or safety of employees or reputation to business. Examples include theft, fraud, assault, being intoxicated at work, or refusing to carry out lawful and reasonable instructions.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

Mere refusal to participate in an internal investigation is unlikely to constitute valid grounds for dismissal.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is common to set out the scope of an investigation before it commences, although this is not mandatory. Consideration should be given to any regulatory compliance obligations, including reporting obligations. It is common for a board of directors to refer an internal investigation to an external adviser, such as a law firm, particularly if the board has concerns about litigation and risk management.

The terms of reference should outline the key allegations or concerns, define the sources of information that it is proposed should be gathered during the investigation, and identify who will report on the findings or recommendations of the investigation and the recipient of the report.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

When a company becomes aware of potential issues, an investigation should be undertaken to identify the nature and extent of any misconduct. Care should be taken in setting up the investigation, including to ensure that communications are confidential and privileged to the extent possible. A company may be obliged to report to regulators in relation to certain breaches, or may elect to self-report or seek immunity. Legal advice should be sought prior to making such decisions as the consequences may be serious. A company should work towards containing the breaches and, as far as possible, secure complete cessation of the offending behaviour. Evidence of the suspected breaches should not be destroyed and document preservation notices should be issued in appropriate circumstances. Any dismissal or discipline of individuals suspected to have participated in the misconduct should be carefully managed and based on legal advice.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Compulsory document production notices must be strictly complied with as it is a criminal offence not to do so without a reasonable excuse. The notice may be addressed to an individual or the 'appropriate officer' within the company. The named individual does not have to coordinate the response but they should be kept informed as they may be held personally liable for any non-compliance.

It is necessary to make 'reasonable endeavours' to respond to a notice. A structured approach to the collation and production of materials should be taken, including where data will be sourced, relevant individuals or custodians of data, document preservation, and how the documents will be collated and stored to preserve original documents and metadata.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

If the internal investigation is confidential, there is no requirement for a company to disclose its existence publicly. Disclosure may be required if it is not possible for the conduct to be contained or if media or market speculation needs to be addressed. If the company is being investigated by regulators, disclosure will often depend on the preferred approach of that regulator. It is usual for regulators to ask that disclosure of the fact of their investigation not be made public unless mutually agreed.

Private companies have no legislative obligation to disclose the existence of an internal investigation or contact from law enforcement.

36 How are internal investigations viewed by local enforcement bodies in your country?

An efficiently run internal investigation is welcomed by the regulator, particularly if it leads to self-reporting. In some circumstances, a regulator may ask the corporate to undertake the first stage of the investigation. If an internal investigation is running concurrently with a regulator's investigation, co-operation in expediting the process and ultimate outcome is encouraged.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Communications made for the dominant purpose of giving or receiving legal advice, or existing or contemplated litigation, can be subject to a legitimate claim for legal professional privilege. If the dominant purpose relates to a factual investigation, it is unlikely that the communication will be privileged.

Lawyers' notes regarding internal investigations are usually protected by legal professional privilege. To protect the privilege, all communications should be marked as confidential and privileged and should not be distributed outside the lawyer–client communication lines unless necessary.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Legal professional privilege is held by the client (company or individual), not the legal adviser. Employees of the company may have grounds to assert common interest privilege, if the employee reasonably believed the lawyer was giving them legal advice and their interests were not adverse to the company. In circumstances where a company seeks to maintain control over the privileged information, lawyers will ordinarily be instructed to communicate that distinction, adopting the US-style *Upjohn* or corporate *Miranda* warnings.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes. The dominant purpose test applies, irrespective of whether the lawyer is internal or external to the company. Best practice is for in-house counsel to hold a current practising certificate and be independent. Privilege claims of advice from in-house counsel generally will be scrutinised, particularly if they hold another non-legal position within the company, or if they are accustomed to providing commercial advice (which will not be privileged).

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Yes. Australian clients can claim the privilege if the communications are with a qualified lawyer admitted to practise in the foreign country and the communications satisfy the dominant purpose test.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

It is normal for companies and individuals to maintain claims of LPP. Waivers are generally restricted to circumstances in which the entity is essentially opening its doors on a no-restrictions basis. It may be considered that not claiming LPP signals an increased level of co-operation with the investigating authority. A court may compel an entity to produce documents if it has determined that the claims for privilege cannot be maintained. However, regulators are increasingly challenging claims for LPP, including taking some matters to court to dispute claims by companies withholding production of documents on the basis of LPP.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Yes. For instance, a party responding to a compulsory notice to produce documents to ASIC may enter into a voluntary confidential LPP disclosure agreement, which allows production of the documents to ASIC, while protecting their disclosure to third parties. ASIC will undertake to treat the information as confidential and will defer to the privilege holder if ASIC is compelled to produce the documents. These agreements have not been tested by the courts as to whether they will withstand a challenge.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Possibly. Relevant considerations will include the context in which the waiver was made (under compulsion or voluntarily), the use of the information subsequent to the waiver and whether, in Australia, privilege would still properly apply to the information.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege does exist. The interest of the parties claiming the privilege must be the same, or almost the same (such that the parties could use the same lawyer), and it will not be available if they are potentially adverse. There is no requirement for a formal agreement between parties to establish this privilege, nor to identify an intention to claim the privilege at the time of communication, although it is advisable to do so to establish the extent of the common interest.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

It is not uncommon for lawyers to brief third-party experts to assist on matters relevant to the giving of legal advice. Communications with the third party will be covered by LPP if they fall within the dominant purpose test.

If a party serves a report or advice prepared by a third party during litigation, all materials (including briefing materials) used by the third party in informing an opinion generally become discoverable. There are limited circumstances in which a party can resist production of communications underpinning a report.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Organisations are permitted to conduct fact-finding interviews during an internal investigation. Consideration ought to be given to ensuring that the individual is afforded the appropriate amount of time to prepare and respond to questions. Whistleblowers, who may be among the first interviewed, are afforded additional legislative protections that must be adhered to.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

LPP can be claimed over witness interviews and reports prepared by legal advisers for the dominant purpose of giving or receiving legal advice or in the preparation of legal proceedings.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Corporate *Miranda* or *Upjohn* warnings are not required to be given, although they are common in cross-border investigations. It is prudent to outline the scope of the lawyer's engagement at the time of the interview, to avoid any misconception as to whether the parties intend privilege to apply. The same approach applies to both current employees or third parties, although there is less scope for privilege to apply to third parties.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

The style of interview will depend on the seriousness of the allegations being investigated. Notes of interviews should be kept confidential and a record of any materials discussed during the interview should be retained for future reference. Generally, a witness will be asked for an independent recollection of events before being presented with any documents. Documents put to a witness should be restricted to those about which the witness has first-hand knowledge. If the allegations are serious and directed to the interviewee, then it is not unusual to provide the interviewee with the option of having their own legal representation at the interview.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

It is mandatory under anti-money laundering and counter-terrorism financing legislation to report suspicious financial transactions to AUSTRAC. The company must have formed a suspicion that the dealings may be related to an offence (such as money laundering, terrorism financing or operating under a false identity, tax evasion or proceeds of crime) and must report within 24 hours if it relates to terrorism, or otherwise three business days.

Australian financial services licensees must report any significant breaches, or anticipated breaches, of obligations under the Corporations Act.

State legislation may also apply.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

If an internal investigation has led to findings of misconduct, a decision will need to be made whether to self-report. Self-reporting may be advisable if the findings are likely to affect the company's ability to conduct its business or trading of the company's shares.

Disclosure to regulators outside Australia may depend on whether the conduct has occurred outside the jurisdiction and the reporting obligations in those other jurisdictions.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

In self-reporting, the company should be prepared to co-operate honestly and completely with authorities and assist regulators' investigations, which may go beyond internal investigation. This will involve providing to authorities any information gathered during the internal investigation at the time of self-reporting.

The company should be prepared to plead guilty to any offence identified and may be required to assist in the prosecution of related parties. Public disclosure will need to be considered for listed companies, consistent with disclosure obligations.

In certain circumstances, immunity for being first-in-time can be sought when reporting to the ACCC.

Legislation allowing deferred prosecution agreements (DPAs) is proceeding through the Australian Parliament. It has been the subject of extensive consultation and is expected to be introduced in late 2019. Once passed, it is anticipated that this legislation will provide benefits to corporates who self-report relevant offences (see question 65).

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Companies take seriously their obligation to comply with notices from regulators. It is possible to enter into a dialogue with a regulator in relation to a notice or subpoena, particularly if there are concerns about scope or time for production. This would be done by speaking or writing to a representative of the regulator in the first instance.

54 Are ongoing authority investigations subject to challenge before the courts?

A company may challenge an investigation if the investigation is an abuse of process or harassment.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Consistency is key when a company is facing allegations of wrongdoing regarding the same facts in multiple jurisdictions. A company should ensure responses are coordinated and that production of documents or information is strictly responsive to the notice. There is no requirement to go beyond the strict terms of the notice and doing so may amount to voluntary disclosure and not be afforded protections (such as confidentiality and privilege) that would otherwise be available.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Materials must be produced if they are in the possession, custody or control of the company in Australia (irrespective of the location where they are held). It may be possible to resist production of materials outside Australia if to do so would be oppressive.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Australian regulators make use of mutual recognition agreements with regulators from other jurisdictions, such as the International Organisation of Securities Commissions. Less formal arrangements exist between some regulators, such as the AFP's arrangements with other police agencies globally. Mutual assistance requests are a formal mechanism by which authorities can obtain information from overseas regulators for use in criminal proceedings.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Information produced under compulsion can only be used for the purpose for which it was obtained. Materials can be shared between regulators, subject to satisfying legislative requirements, and can be disclosed to third parties during an investigation if it is deemed necessary.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Refusing to produce a document that is disclosable under the notice will be a breach and may give rise to legal action by the regulator. Open dialogue with the regulator is encouraged at an early stage to attempt to negotiate an amendment to the notice to exclude production of documents that give rise to a breach of laws in another jurisdiction. Otherwise, the company should look at avenues to challenge the notice.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Australian data privacy laws prevent the disclosure of certain personal and sensitive information. The APPs apply to government agencies, private sector and not-for-profit organisations (with an annual turnover of more than A$3 million), private health providers and small businesses.

Disclosure is permitted if compelled (such as by a document production notice or subpoena) or reasonably necessary for one or more enforcement-related activities by an enforcement body. In defending allegations of misconduct, data may also be transferred for the purposes of, or in connection with, legal proceedings (including prospective legal proceedings) or for the purposes of establishing, exercising or defending legal rights.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

It is common for companies to request that a regulator issue a notice to compel the production of materials to preserve claims of confidentiality and privilege. Such a claim may be

waived by voluntary production. Regulators can be compelled to produce documents to third parties by court order, but may segregate documents that are subject to claims of privilege (including LPP and public interest immunity) and confidentiality, and leave it to the court to rule on such claims.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Companies can face financial penalties, which can be up to 10 times what is imposed on an individual, or more for offences for which penalties are based on company turnover.

Penalties against an individual will vary depending on the offence. Criminal wrongdoing may result in imprisonment or financial penalties, or both. Civil penalty proceedings can result in fines, compensation orders and disqualification from managing corporations.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

The Commonwealth and state/territory government does not automatically suspend or disbar a company for any conduct, although it does have discretion to preclude a company from public procurement contracts.

64 What do the authorities in your country take into account when fixing penalties?

Courts will consider a range of factors, including the seriousness of the offence, the number of contraventions and the period during which they occurred, the need for general deterrence, remorse, retribution, co-operation and any relevant personal circumstances.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

DPAs are not currently available but are likely to be introduced in the near future (see question 52). Based on the current proposed legislation, DPAs will allow companies to negotiate terms of settlement for allegations of serious corporate crime, which include the setting of a penalty for contravention, but will require approval by an approving officer before they can be finalised. Not all corporate crimes are covered in the proposed legislation and DPAs will not be available to individuals.

DPAs under the proposed incoming legislation are similar to non-prosecution agreements under US law.

Another mechanism in which a company may reach agreement with authorities to avoid prosecution in return for co-operation is by seeking an indemnity, more formally referred to as an undertaking, under the Director of Public Prosecutions Act 1983 (Cth). The circumstances in which an indemnity may be granted are generally governed by the Prosecution

Policy of the Commonwealth. In the context of cartel prosecutions, applications are governed by the ACCC Immunity and Cooperation Policy for Cartel Conduct.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

There is no certainty regarding implementation of DPAs in Australia at present; however, the proposal is that the DPA be published in full, except in exceptional circumstances, such as when the publication would prejudice court proceedings. This approach would be consistent with that taken when a company has pleaded guilty, or been granted an indemnity for prosecution, but proceedings are also under way against connected individuals or corporate entities (for instance in the case of cartel proceedings).

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Considerations relevant to settlement include an assessment of the facts and allegations made against the company, the strength of the evidence, the terms on which the regulator is willing to settle (where they can be agreed) and the potential consequences of any settlement (including on business operations, investigations in other jurisdictions and the risk of collateral civil litigation).

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

The proposed DPA process suggests the use of an independent monitor, paid for by the company, to assess compliance with the terms of the DPA. The reason for this is, in part, that the body responsible for entering into DPAs with companies, the CDPP, does not have a monitoring function. External corporate compliance monitors have also often had a role in enforceable undertakings with ASIC.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Private actions are permitted to run in parallel with criminal or regulatory proceedings, provided they do not prejudice the accused's right to a fair trial, or the right to maintain privilege against self-incrimination or exposure to penalty, and do not interfere with the criminal proceedings. It is common for private or civil actions to be stayed pending the outcome of criminal proceedings.

Private plaintiffs are entitled to apply to regulators to access files through various mechanisms, including Freedom of Information requests and subpoenas. In addition, ASIC has the power to provide information to private litigants in certain circumstances. The disclosure of information by regulatory bodies is subject to overriding considerations of public interest, the risk of prejudice to an ongoing investigation or proceeding, and statutory restrictions.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Criminal investigations are generally confidential. An accused has the right to a fair trial and a presumption of innocence. Investigatory bodies, such as the AFP, have media policies that restrict the publication of information that may prejudice an ongoing investigation or affect an accused's right to a fair trial, particularly in tainting the jury pool.

Criminal court proceedings are a matter of public record. There are limited situations in which a corporation or individual can restrict access to, or publication of, the court proceedings. Although the media are entitled to report on public hearings, they are required to follow orders from the judge relating to non-publication of certain information. Jury deliberations are confidential. It is an offence to publish anything regarding the identity of a juror or the discussions that take place in the jury room.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common for public relations firms to be hired, particularly in high-profile matters. Lawyers will generally work with a public relations firm to ensure accuracy of reporting and in making any public statements during an investigation or proceeding.

72 How is publicity managed when there are ongoing related proceedings?

Corporations need to carefully manage the release of information regarding ongoing proceedings to avoid being in contempt of the proceedings or prejudicing the proceedings, especially any criminal proceedings before a jury, and to meet any relevant continuous disclosure obligations. Regulators will announce the commencement of proceedings and may provide procedural updates but generally will not comment on substantive matters for the duration of the proceeding.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

If the settlement is likely to have a material effect on the price or value of the company's securities and does not fall within an exception (such as the information being confidential), it is required to be disclosed to the market by a public company. Confidentiality alone is not grounds for non-disclosure of the fact of settlement. It is often the case that parties agree the terms of disclosure of a settlement as part of the settlement negotiations.

Anticipated developments

74 **Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?**

The outworking of the BRC is likely to result in a higher volume of civil penalty proceedings and criminal proceedings against companies and individuals arising from investigations by regulatory bodies such as ASIC and the Australian Financial Complaints Authority (which provides a dispute resolution mechanism for consumers). Consequential civil litigation is likely to arise in the form of class actions or other private civil actions, in which individuals and organisations seek to make use of the regulators' more public and aggressive enforcement approach.

7

Austria

Bettina Knoetzl and Thomas Voppichler[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Since 2017, a wide-ranging investigation of the construction sector has been pending in Austria. Currently, the authorities involved are assuming that the companies concerned have colluded on up to 800 construction projects. In most cases, the projects were administered by public authorities who were required by law to invite tenders for their public works. The cost of the construction projects is estimated at several hundred million euros.

The Central Public Prosecutor's Office for Economic Crimes and Corruption (WKStA) and the Austrian Federal Competition Authority are involved in the investigation. Following the first raids in 2017, and further raids in 2018, around 60 companies and more than 150 individuals are now subject to prosecution. To date, the authorities have seized more than 70,000 pages of documents and 57 terabytes of IT data.

While it is currently assumed that the criminal proceedings conducted by the WKStA (natural persons face a prison sentence of up to 10 years, companies face fines of up to €1.3 million) will still take several years before indictments are filed, the Federal Competition Authority announced the first applications for fines by the turn of the year. Antitrust behaviour may be sanctioned with fines of up to 10 per cent of a corporate entity's total turnover.

2 Outline the legal framework for corporate liability in your country.

The Austrian legal system distinguishes between civil liability (for breaches of private law), criminal liability (for offences against criminal law) and liability under administrative

1 Bettina Knoetzl is a partner and Thomas Voppichler is a counsel at KNOETZL.

penal law (for regulatory offences). The main focus of this chapter is on criminal liability of corporations.

Pursuant to the Law on Corporate Liability (VbVG), corporations are liable for the unlawful and culpable actions of their decision makers and, under more restrictive conditions, for the actions of their employees, provided that the offence was either committed for the benefit of the corporation or the offence violated duties incumbent on the corporation. Moreover, an offence committed by an employee must have been either rendered possible or facilitated by the decision makers' failure to take essential precautionary measures, in particular of a technical, organisational or personal character.

In contrast to the liability for criminal offences, corporations are only directly liable for regulatory (administrative law) offences against tax law (section 28a, Penal Tax Code). In other areas of administrative penal law, there is only an indirect joint liability of the corporation for fines imposed for offences committed by the managing director or other 'persons in charge' (section 9, Administrative Penal Code). However, these offences are considered offences by the natural person, not the corporation.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Criminal offences are investigated by public prosecutors with the assistance of the criminal investigation department of the police. Pursuant to section 20a of the Code of Criminal Procedure (StPO), the WKStA is responsible for prosecuting economic crimes and corruption. The Federal Bureau of Anti-Corruption assists the WKStA in matters relating to corruption.

Administrative law is enforced by various administrative authorities, often with sector-specific competences. The most notable examples are the Financial Market Authority, which oversees, inter alia, banks, insurance companies and companies listed at the Vienna Stock Exchange, and the Competition Authority, which conducts investigations into possible violations of national and European competition law.

Although competences between criminal and administrative authorities are distinguished *ratione materiae*, situations can arise in which different authorities have parallel competence over the same facts. Pursuant to section 15 of the StPO, criminal courts must autonomously decide preliminary questions pertaining to other areas of law. However, they may await the decision of a competent court or administrative authority on such preliminary questions if the decision is to be expected in the foreseeable future. Administrative authorities, in turn, may suspend their investigations if a preliminary question forms the object of another proceeding.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Yes, for the opening of a criminal investigation, an 'initial suspicion' is required. Pursuant to section 1, paragraph 3 of the StPO, this is the case whenever specific indications give reason to suspect that a criminal offence has been committed.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Persons suspected of a crime have a right against self-incrimination (see question 27). However, non-compliance with a notice to produce documents or a subpoena to appear before the investigation authority may lead to coercive measures, such as house searches. A coercive measure can be challenged by means of a complaint, arguing, for example, that the measure violates the principle of proportionality (section 87, StPO). If documents are protected by attorney–client confidentiality, an objection to the temporary securing can be filed and the sealing of the documents or data can be requested, to obtain a court decision to release the data (see question 26).

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

See questions 28 and 51. The intention of the leniency programme is to promote assistance from the perpetrator of a crime, to detect and prosecute other crimes that could otherwise not, or only with great difficulty, be investigated. In this way, both the state and the perpetrator derive benefit from the leniency programme.

7 What are the top priorities for your country's law enforcement authorities?

Fighting corruption is an express priority of the current government, more specifically the Austrian Ministry of Justice. Since Austria's ratification of the UN Convention Against Corruption in January 2006, a – more or less – constant improvement of the anti-corruption laws could be observed. A number of legislative improvements have been implemented to fight corruption, including the creation of the Federal Bureau of Anti-Corruption in 2010 and the WKStA in 2011 (see question 3).

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

The Austrian Act on Security of Network and Information Systems (NISG) was enacted in 2018 to implement the corresponding EU Directive (2016/1148 concerning measures for a high common level of security of network and information systems) as the first EU-wide regulation on cybersecurity. It obliges companies to establish comprehensive security measures and to prove their effectiveness. Failure to comply with the requirements of the NISG could result in penalties and loss of reputation. The focus of the NISG is on operators of essential services that are of major importance, in particular for the maintenance of public health services, the public supply of water, energy and vital goods, public transport, and the functionality of public information and communication technology, the availability of which depends on network and information systems.

Additionally, the General Data Protection Regulation (GDPR) must be considered in connection with requirements of cybersecurity (see question 22).

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

In 2013, the European Parliament enacted Directive 2013/40/EU on attacks against information systems, which was incorporated as part of Austrian national (criminal) law in 2015. The Directive seeks to 'approximate the criminal law' in the area of cybercrime and to improve co-operation between competent authorities.

Moreover, a cybercrime competence centre to combat computer crime was set up as a separate unit within the Austrian Federal Criminal Police Office. The cross-border prosecution of computer-related crime in the European Union is coordinated by the European Cybercrime Centre, set up by Europol.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Austrian criminal law has no general extraterritorial effect (section 62 of the Austrian Penal Code (StGB)). Criminal offences committed on an Austrian ship or aeroplane are subject to the StGB, as are certain offences regardless of the criminal law of the location of the offence, including economic espionage, criminal offences against an Austrian official, human trafficking, terrorism, corruption and several other types of major crimes (section 64, StGB).

Other offences committed abroad are only subject to Austrian criminal law (1) if the offence is also punishable under the laws of the place where the offence is committed, (2) if the offender is Austrian or is arrested in Austria and cannot be extradited, and (3) none of the exceptions set out in section 65(2)4 of the StGB applies.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The co-operation between Austrian prosecutors and their counterparts in other EU Member States is greatly facilitated by three instruments: the European evidence warrant, the European investigation order (EIO) and joint investigation teams (JITs). Hereafter, the focus of our discussion is on the latter two. Also of relevance is the Law on Judicial Cooperation in Criminal Matters.

The EIO replaces the classic system of judicial assistance, as it allows the competent authority of one EU Member State (the issuing state) to order, after validation by a court or public prosecutor of the issuing state, the execution of most acts of investigation, including coercive measures, in another EU Member State (the executing state) (Article 2, Directive 2014/41/EU of 3 April 2014). Subject to certain grounds for non-recognition, non-execution or postponement, the executing state must ensure the execution of the order as if the investigative measure concerned had been ordered by a domestic authority (Article 9, Directive 2014/41/EU). The national law of the executing state may provide that authorisation by a domestic court is required (Article 2(d), Directive 2014/41/EU). When this is not the case, the EIO may be directly executed by the executing authority.

JITs are multinational investigation teams based on an agreement between two or more law enforcement authorities in EU Member States and are set up to investigate a specific matter for a fixed period. The co-operation can be extended to non-EU Member States if all other participating parties agree.

By contrast, the co-operation between Austrian prosecution authorities and non-EU Member States (and Denmark) still follows traditional judicial assistance practice based on the principle of reciprocity and governed by international agreements and, when these do not contain a governing rule, the Extradition and Judicial Assistance Law, which only applies in ongoing criminal proceedings in Austria; it does not apply to administrative proceedings. Unless an international agreement provides for direct judicial assistance, the Austrian authorities must request judicial assistance through the Federal Ministry of Justice. Moreover, unlike in an EIO, the public prosecutors must request and obtain court authorisation from the domestic court for coercive investigation measures.

Finally, special challenges arise when investigations relate to countries with strong secrecy rules, for example Swiss banking secrecy.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The transnational effect of the *ne bis in idem* principle (established in section 17(1), StPO) is based on international agreements to which Austria is a party (see Alois Birklbauer in Fuchs and Ratz, *Wiener Kommentar zur Strafprozessordnung*, section 17). Of particular importance for the transnational effect of the principle is Article 54 of the Convention implementing the Schengen Agreement (the implementing Convention), which prohibits prosecution for 'the same offence', if a person has been 'finally judged' and has already served, or is serving, a sentence in another contracting state (note that Austria has made declarations relating to all exceptions enumerated in Article 55 of the implementing Convention).

In the context of Article 54 of the implementing Convention, Austrian authorities apply different concepts of 'same offence' to different situations. For a criminal court, confronted with a previous sentence of another criminal court, the previous sentence deploys a blocking effect in relation to the same factual matrix. This concept is favourable for the accused. By contrast, a criminal court can convict an accused on the same facts if the accused was previously sanctioned by an administrative authority (rather than a criminal court) and the sanction did not fully correct the injustice done.

Article 54 of the implementing Convention speaks of a person who has been 'finally judged'. According to both case law and legal scholarship, the concept of final judgment encompasses all judgments that conclude a main trial, namely both convictions and acquittals. No differentiation is made by the Court of Justice of the European Union (CJEU) between an acquittal based on a judgment on the merits or a procedural judgment. Moreover, the closure of proceedings by the prosecution authority without the involvement of a court has a blocking effect for the purpose of Article 54 of the implementing Convention if it is the result of an action for compensation (in Austria, this is called diversion – see question 51)

brought by the person under investigation and the closure is final (*Gözütok and Brügge*, CJEU judgment of 11 February 2003, C-187/01, C-385/01). Other provisions dealing with previous convictions abroad are section 192 of the StPO and section 66 of the Austrian Penal Code (StGB).

A further provision entitling criminal prosecutors to refrain from prosecution is contained in section 192(1) of the StPO (which applies in cases falling outside the scope of the implementing Convention or other international agreements), provided that the suspected person is charged with several offences, the person has already been convicted by a foreign court for the offence, or the person has made compensation abroad and as a result has been exempted from further prosecution (diversion), and no more severe penalty is to be expected in Austria. Finally, pursuant to section 66 of the StGB, Austrian courts must take into account a punishment for the same crime imposed and served abroad. Otherwise, the Austrian legal system does not provide for a 'anti-piling on' policy.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not common in Austria. For the effect of a diversion in EU Member States, see question 12.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

See question 12, and paragraph 17 of the Preamble to Directive 2014/41/EU regarding the European investigation order in criminal matters, which allows an EIO aiming 'to establish whether a possible conflict with the *ne bis in idem* principle exists'.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Austria itself has not imposed any sanctions against other states. However, for the Austrian economy, the sanctions imposed by the European Union on various states, for example in connection with Syria or Russia, must be considered.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Parallel to the (primarily) EU sanctions that should be taken into account, a supplementary Austrian Sanctions Act (SanktG) is in force, which regulates, for example, domestic implementing measures of sanctions of the European Union or the United Nations and penal provisions relating to any violation of imposed sanctions.

According to published crime statistics, there has been no conviction under the SanktG – which is only a subsidiary offence – in recent years.

There has been no apparent increase in the enforcement of sanctions violations, based on publicly available information.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Yes. The co-operation is based on the existing European legal instruments (see question 11).

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Austria, itself, has not enacted any blocking legislation. However, see question 60 regarding Council Regulation (EC) No. 2271/96 protecting against the effects of the extraterritorial application of legislation adopted by a third country (the Blocking Statute).

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Austria, itself, has not enacted any blocking legislation. However, see question 60 regarding the Blocking Statute.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Occasionally, allegations of misconduct arise out of tax audits. It is also not infrequent that competitors and victims of misconduct bring unlawful conduct to the attention of the authorities. Other common ways are chance discoveries of an offence, whistleblowers, standard screening processes, suspicious activity reports, internal audits, tax reporting, compliance and media reports.

Information gathering

21 Does your country have a data protection regime?

EU regulations on data protection – with their usual high standards – are applicable in Austria. The GDPR, which is directly applicable in all EU Member States, became effective on 25 May 2018. In addition to the GDPR regime, the Austrian Law on Data Protection (DSG) has further provisions on data protection, and on institutional and procedural aspects.

Personal data is defined as any information relating to an identified or identifiable natural person (see Article 4, GDPR). When it comes to the processing of personal data during an internal investigation, companies must comply with GDPR stipulations. According to Article 5 of the GDPR, personal data shall be collected only for specific, explicit and legitimate purposes and, inter alia, be processed lawfully, fairly and transparently. In that regard, the processing of personal data is lawful only if the data subject has given consent and if it is necessary, inter alia, for:

- the performance of a contract or responds to the data subject's request prior to entering a contract;

- compliance with a legal obligation to which the data's controller is subject; or
- the purpose of the legitimate interests of the data's controller (see Article 6, GDPR).

Moreover, the GDPR provides for a catalogue of rights applicable to data subjects, including the right to be informed about the processing and storage of personal data, the purpose of data processing and the duration of storage. Furthermore, the GDPR provides for a data subject's right to file a complaint with the relevant supervisory authority (see question 22) if the processing of personal data may have violated data protection rights.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

As is widely known, infringements of GDPR provisions are sanctioned by severe administrative fines, which can amount to €20 million or 4 per cent of the corporation's annual global turnover, whichever is higher. Implementing the GDPR provisions, Austria's Data Protection Authority (DSB) was established to monitor the application of the Regulation and, as Austria's supervisory public authority, is competent to enforce GDPR provisions.

As an exceptional measure in implementing GDPR provisions, the Austrian legislature added its own provision regarding the DSB's use of corrective powers (see Article 58, GDPR). According to section 11 of the DSG, the DSB shall make use of its corrective powers under Article 58 of the GDPR, particularly in the case of first-time infringements, primarily by issuing warnings. Since the GDPR does not entitle EU Member States to direct supervisory authorities on how to exercise their powers, this provision may violate the DSB's independence, under Article 52 of the GDPR.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

As in all EU Member States, GDPR provisions must be considered carefully when data is processed. The term 'processing' is defined as any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation upon, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (see Article 4, GDPR).

During an internal investigation, a considerable amount of evidence, including personal data, will be processed by collecting, storing, using, disclosing, etc. To comply with GDPR provisions, it should be well documented which data is classified as personal and which as non-personal. Furthermore, investigating companies should document in detail the purpose of processing personal data and comply with GDPR provisions regarding storage limitations, integrity and confidentiality. Besides that, companies should be especially careful when it comes to transnational data transfers, especially from or to non-EU Member States.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Private email accounts or telephone conversations may not be monitored by the employer under any circumstances.

The protection of the employee's privacy must also be observed regarding professional emails or telephone calls. Monitoring affects human dignity and triggers the employee's or works council's obligation to give his or her prior consent. The obligation of pre-approval does not depend on whether the private use of the professional email account or internet connection is permitted by the employer; it applies in every case, unless higher interests justify the screening of the company's data. In any event, the GDPR must be considered (see question 21).

Affected employees can assert injunctive relief claims and, if necessary, contact the DSB (see question 22).

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

With the approval of the court, the public prosecutor may order the search of a specific location – for instance, an office building – to collect, temporarily secure or seize evidence, or any kind of assets that may serve as evidence, not only for the subsequent phases of the proceedings but also for the sole purpose of securing civil claims of parties injured by the (alleged) criminal offence (section 119(1), StPO). In cases in which there is a risk that by waiting for a court order the evidence may become unavailable, the public prosecutor may order the search of a location before seeking court approval (section 120, StPO).

Persons in possession of documents, data carriers or assets that form the object of a request for temporary securing are under a legal duty to comply unless they are suspected of the underlying offence or discharged from testifying, or have a right to refuse to give evidence (section 111, StPO). However, the public prosecutor can obtain the evidence by coercive means, such as a house search. Regarding the protection of privileged material, see question 26.

In addition to prior or subsequent court approval, house searches are subject to certain prerequisites. Most importantly, there must be a founded suspicion (this threshold is higher than the initial suspicion required to open investigations – see question 4) and the coercive measure needs to comply with the principle of proportionality. A temporary securing or seizure is not lawful if a less intrusive means is available (for instance by photocopying documents – see section 110(4), StPO).

Persons against whom a search warrant was issued, or whose premises have been subject to a search, can file an objection with the competent public prosecutor within six weeks of the measure (section 106 StPO). The public prosecutor can either comply with the objection or, within four weeks, pass the objection to the competent criminal court.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Attorney work-product and attorney–client communications are protected in several ways. Attorneys (and a small number of other professions) have a legal duty of confidentiality and

a right to refuse to give evidence (section 157, StPO). The duty may not be circumvented. This prohibits the seizure of attorney documents and the information contained therein at the attorney's premises and, since November 2016, also at the premises of clients under suspicion or accused in criminal proceedings. The attorney–client confidentiality only extends to the attorney's work-product and attorney–client communications created for the purpose of defending the client and not to previously existing evidence.

Any person subject to or present during a measure of temporary securing may object to the temporary securing of material protected by attorney–client confidentiality (sections 106 and 115, StPO). In the case of such an objection, documents and data carriers have to be sealed and presented to a court, which must decide promptly whether the evidence is protected (section 112, StPO).

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Accused individuals or companies have a right to avoid self-incrimination. In the case of a corporation, the managers (persons in charge) and the employees suspected of having committed an offence are to be interrogated as accused (section 17(1), VbVG). It is forbidden to use coercive measures (or promises or misleading statements) to induce the accused to make a statement (section 7(2), StPO). Pursuant to section 166 of the StPO, compelled testimony is classed as prohibited evidence and is null and void.

Relatives of the accused are discharged from the duty to testify (section 156(1)1, StPO) and witnesses can refuse to testify if they would incriminate themselves or expose a relative to the risk of criminal prosecution (section 157(1)1, StPO). On attorney–client confidentiality, see questions 26 and 38.

Privileges exist for members of certain professions, such as lawyers, auditors, medical doctors, psychiatrists, mediators, priests and reporters (section 157, StPO).

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Whistleblowers can bring alleged offences anonymously to the attention of the WKStA through a whistleblower website, for which a legal basis was created in 2015.

A whistleblower may benefit from the crown witness regulation (section 209a, StPO). This regulation concerns serious offences and is available, if the witness freely confesses his or her contribution to the offence, if the information disclosed is new and not yet part of an investigation against the witness, and if it contributes substantially to the investigation. Subject to further prerequisites (section 209a, StPO), criminal prosecutors may terminate the investigations against such a person, for example in return for payment of a monetary contribution. This will generally be less than a fine imposed by the court in the event of a conviction, which can also create a financial incentive.

Similarly, section 11b of the Austrian Act on the Establishment of a Competition Law Authority also contains a crown witness regulation. Other provisions on whistleblowing are contained in section 160 of the Federal Law on the Stock Exchange 2018 (BoerseG).

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employers have a duty of care towards their employees, including those in an executive or managerial position (section 1157(1), Austrian Civil Code; section 18(4), Law on Employees (AngG). Pursuant to this duty, the employer must, inter alia, respect the private life of employees, protect their honour and treat them equally. This also has an effect on the conduct of internal investigations. Prior to an interview, the employer (or third party acting for the employer) should, for instance, inform employees that they may be accompanied by their own legal representative, at least in situations of a (potential) conflict of interest. For protection provided by other branches of law, see question 48.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

A finding of misconduct will frequently destroy the trustworthiness of an employee and justify dismissal. However, a mere suspicion of a criminal offence is insufficient. Stricter standards apply to employees in executive positions (Decision of the Austrian Supreme Court, RS0029652).

Under Austrian law, an employer may only dismiss an employee without giving notice if the employer exercises this right immediately after becoming aware of the reason justifying the dismissal (Decision of the Austrian Supreme Court, RS0029131). Employers forfeit this right if they fail to exercise it immediately (a requirement that has proved controversial in cases of a suspected criminal offence – see Silke Heinz-Ofner in *AngG: Angestelltengesetz – Kommentar*, Reissner (editor), 2nd edition, section 27, No. 52). If there is any doubt, an employer can suspend an employee until the investigation yields more evidence.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

Employees have a duty of loyalty to their employer and a duty to inform (for the employer's corresponding duty of care, see question 29). Whether this duty gives rise to an obligation to answer the questions of private investigators that may reveal personal misconduct is a matter of controversy in Austrian scholarship. On the one hand, it is recognised that the right against self-incrimination is only applicable as regards state authorities. On the other, it has been argued that an employee must have some right against self-incrimination, if the internal investigation forms a prelude to criminal investigation, since the employee would otherwise be effectively deprived of his or her defence rights in criminal proceedings (see, for example, Ingeborg Zerbes, 'Strafrechtliche Grundsatzfragen "interner Untersuchungen"',

Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2013, 263, at pages 271 and 272). To our knowledge, the matter has not yet been decided by a court.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Austrian corporations follow the international practice of setting out the terms and the personal, material and temporal scope of an internal investigation in a document. The issues usually covered include:

- person acting as internal investigator;
- definition of types of documents and electronic data (correspondence, documents) and method of screening;
- internal or external interviewers;
- persons to be interviewed;
- definition of documents or (provisional) outcomes of the internal investigation with which the interviewees will be confronted;
- channels of communication;
- involvement of an accounting department;
- definition of spheres of confidentiality;
- phases of the internal investigation;
- point in time of informing persons whose data is used; and
- treatment of data during and after completion of the investigation.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

In principle, companies are under no legal duty to bring misconduct to the attention of enforcement authorities. Doing so can allow a company to benefit from the crown witness regulation (see question 28) or from gaining 'victim status' (as an injured party) rather than being treated as a suspect in the proceedings. Reporting duties can arise from rules on corporate governance and company law, depending on a company's size and other relevant factors (see, notably, the requirement of a status report pursuant to section 243 et seq. of the Austrian Commercial Code). Managing directors of public limited companies must report to the president of the supervisory board any violations, or any suspicions of violations, that are of significant consequence to the company, and managing directors of limited liability companies have a corresponding duty to report to the shareholders.

See also question 73 regarding the duty of publicly listed companies to issue ad hoc notifications.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

As a general rule, everyone is under a legal duty not to destroy material that may become relevant in a legal dispute. Suppression of evidence is a criminal offence (section 229, StGB).

Advisable measures include the search and preservation of relevant data and the drawing up of an internal memo recording the findings. Companies should also review the settings of deletion routine and instruct employees not to delete any emails, nor to destroy relevant data.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

See questions 33 and 73.

36 How are internal investigations viewed by local enforcement bodies in your country?

The views of local enforcers can vary. Internal investigations may be regarded as helpful, especially if the results are shared with the prosecution, or as a fig leaf that obfuscates rather than assists the criminal investigation. The sharing of the results of an internal investigation may be taken into account as a factor leading criminal prosecutors to refrain from prosecution (section 18, VbVG – see also question 51).

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

If an attorney is conducting an internal investigation or mandates a third party (see question 45), products such as investigation reports are covered by attorney–client confidentiality (see question 26). It is recommended to store attorney work-product so that the data continues to belong to the attorney, for example using only a SharePoint provided by the attorney. In this way, objections and challenges in the case of a house search at a client's or third party's premises can be avoided.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The holder of the confidentiality obligation is the attorney. He or she owes it to the client and the client may release the attorney from the duty. However, attorneys are under no duty to testify. Even if the attorney is released from the duty of confidentiality by the client, he or she still must consider the potential to cause damage to the client when testifying and, if required, refrain from testifying. If, on balance, a refusal to testify serves an attorney's client's interests better, he or she is under a duty not to testify. The confidentiality obligation applies regardless of whether the client is an individual or a company.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The attorney–client privilege applies only to external counsel.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Section 157 of the StPO (see question 26) stipulates that lawyers are entitled to withhold testimony. This applies to Austrian lawyers and to lawyers from other European countries who can work in Austria as service providers or as European lawyers in private practice in accordance with EIRAG (Federal Act on the Free Movement of Services and the Establishment of European Lawyers and the Provision of Legal Services by Internationally Active Lawyers in Austria). It has not yet been decided whether a non-European lawyer may also invoke the obligation of confidentiality under Austrian law in Austrian proceedings. In our opinion, this would have to be permissible otherwise the procedural right of the accused client to avoid self-incrimination could be circumvented. In practice, Austrian courts respect the right of a private practitioner to refrain from testifying against the interests of a client.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

There is a general understanding that waiver of the attorney–client privilege is necessary to obtain co-operation credit. However, no legal rule exists that would render a waiver mandatory. As noted under question 38, attorneys may be under a duty to insist on confidentiality even if a client has discharged them from it.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

It is not possible to limit disclosure of information to the prosecuting authority for the whole duration of the proceedings. The prosecuting authority must share relevant information with the parties who have access to the criminal file. It can only grant confidentiality for a limited period but will ultimately have to disclose it.

Accused or suspected persons may release their attorneys with regard to certain aspects of the facts only. As explained in questions 38 and 41, attorneys are under no obligation to testify, even if they are released from their duty of confidentiality.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

There is no legal requirement in Austria to waive attorney–client confidentiality. However, if information is in the public domain, it is no longer protected. If information is made part of the criminal file, the prosecution may restrict access only for a limited time.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Given the fundamental difference between the discovery provisions under Austrian law and those applicable in common law jurisdictions, there is no need for a US-style concept of common interest privilege.

Third parties to whom information was disclosed may not have a duty to keep the information confidential or may not benefit from a right to refuse to testify.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Where it is necessary for an attorney to resort to third parties (e.g., a forensic or accounting expert) for the purpose of carrying out his or her own mandate, these third parties are considered as assistants of the attorney and information they obtain or the work-product they produce is confidential (section 9(3), Law on Attorneys; see also Alexander Tipold and Ingeborg Zerbes in Fuchs and Ratz, *Wiener Kommentar zur Strafprozessordnung*, sections 110 to 115, No. 30).

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes. Based on their duty of loyalty, employees must participate in such interviews (for limitations, see questions 29, 30 and 31). If the interview is conducted by an Austrian lawyer, he or she must refrain from influencing the witness' future statements.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

There is no case law confirming that attorney–client confidentiality covers interviews conducted by, or reports drafted by, attorneys on the instruction of their client. However, based on the general principles outlined in questions 26 and 37, it must be presumed that such information is protected. The attorney–client privilege applies in the same way regardless of whether the client is an individual or a company.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Any interview has to be conducted within the confines set by law, notably the employer's duty of care towards its employees (see question 29), the protection of privacy, substantive criminal law and data protection law. Data protection law requires, inter alia, the respect of the principle of proportionality in using data. In most situations, recording the interview will require the agreement of the interviewee, but may also be justified by the prevailing interests of the company (section 12(2), DSG).

Whether further legal restrictions apply, in particular the right against self-incrimination, is subject to debate in Austria (see question 31). As long as the current legal uncertainty persists, it seems advisable to at least inform interviewees of their potential right against

self-incrimination and their right to legal representation. There is no duty of care between a company and third parties who are not employees.

If the interview is conducted by an attorney, the attorney will have to comply with the attorneys' code of conduct. This requires the attorney to inform the interviewee about the capacity in which he or she is acting and by whom he or she was instructed. Attorneys conducting interviews are required, moreover, to avoid influencing the witness' future statements.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Interviews are usually conducted by two interviewers with the help of a questionnaire. It is common that a written record is taken of the interview. Less frequently, interviews are recorded (see question 48). Depending on the circumstances, the interviewee may be presented with documents. Especially in the case of a potential conflict of interest between the interviewee and the interviewer or company, an employee may be accompanied by his or her own legal representative (see question 48).

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

There is no legal duty for private companies to report misconduct to law enforcement authorities. There may be such a duty for state companies exercising sovereign power.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting may be advisable in circumstances in which the company can take advantage of a leniency programme, such as through the crown witness regulation (see question 28) or the diversion procedure, or to gain victim status in the proceedings (as an injured party) rather than facing the risk of accusation.

Diversion in relation to corporations is regulated in section 19 of the VbVG. Pursuant to this provision, the public prosecutor must close a criminal prosecution against a corporation if certain requirements are met. These include that the alleged offence is liable to *ex officio* prosecution, the facts of the case are sufficiently established (here self-reporting may be essential), the personal culpability of the accused is not grave, the consequences of the alleged wrongdoing was appropriately compensated by the payment of damages, and the punishment of the corporation is necessary for reasons neither of special nor of general prevention.

Moreover, dropping charges pursuant to section 19 of the VbVG is subsidiary to section 18 of the VbVG, which entitles public prosecutors to close a criminal prosecution against a corporation if punishment seems unnecessary considering a number of factors, including the conduct of the corporation after the alleged offence (here self-reporting may

again be of particular importance), the seriousness of the alleged offence, the amount of the fine to be imposed, and the detriment suffered by the corporation owing to the misconduct.

To take advantage of the leniency programme, it is important, inter alia, to self-report before the criminal prosecution becomes aware of the alleged misconduct. The disclosure should include all companies and persons who are to benefit from the leniency programme. Owing to the complexity of the procedural rules, it is highly recommended to engage a local lawyer to secure the benefits of such a programme.

In cases involving misconduct in several countries, the advice will have to take into account the principle of *ne bis in idem*. It is essential to form a strategy considering all countries having criminal or regulatory jurisdiction over the case simultaneously.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

See question 51. In any event, a local lawyer who specialises in business crime law should be engaged before taking any practical steps of self-reporting in Austria. The disclosure can be made anonymously, using, for example, the WKStA's whistleblowing tool, or openly by providing the names of all involved parties, as is especially the case when seeking leniency.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Companies should immediately inform their attorney of a notice or subpoena and should, in most cases, seek to enter into a dialogue with the law enforcement authority. In most instances, this will be initiated by calling the authority to arrange a meeting between the company and its attorney at the authority's offices.

54 Are ongoing authority investigations subject to challenge before the courts?

The only remedy to challenge an ongoing investigation is a motion to terminate the prosecution (*Einstellungsantrag*), which can be filed with the public prosecutors, at the earliest, three months after the opening of the investigation (section 108, StPO). The public prosecution may either close the prosecution or pass the motion to the court, with an (optional) statement of its position. Generally, the motion is likely to succeed if it is filed with the blessing of the authority or even if an initial suspicion is lacking. However, if the authority is of the opinion that further facts need to be clarified, the court would usually allow the investigation to continue and dismiss the motion.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

The company may regard the two proceedings as separate and handle them separately. However, a negotiation of disclosure packages with authorities from various countries is

advisable, especially if the prosecution teams co-operate closely. In any event, companies are well advised to safeguard consistency.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Companies are not required to search for and produce material, whether they are located in Austria or abroad. Orders for temporary securing of evidence (see question 25) can extend to documents abroad, but require either traditional judicial assistance or, between EU Member States, an EIO (see question 11).

Although there is no obligation, it may be advisable for a company to search for documents and produce them to avoid coercive measures, such as house searches.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

See question 11.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Austrian officials may not disclose any secret entrusted or accessible to them by virtue of their office (section 310, StGB). In practice, leaks to the public are quite common in Austria as soon as a more extensive number of parties have access to the criminal file (see question 42). In addition, in cases of public interest, the authorities are expressly required to keep the public informed (see also question 70 concerning the Media Decree of the Ministry of Justice). This duty to inform compromises the duty of confidentiality to a certain extent.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

If the company does not want to disclose the document, we would advise the public prosecutors that our client is not entitled to disclose the document. If the company prefers to disclose the document, we would inform the public prosecutors that they have to resort to coercive measures based on judicial assistance or an EIO to obtain the document in the country where the document is located (see question 11).

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

On 7 August 2018, the European Union enacted an updated Blocking Statute to nullify US sanctions on countries trading with Iran, after the US announced sanctions against those countries following its withdrawal from an agreement permitting trade if Iran curtailed its

nuclear programme. The 2018 Blocking Statute essentially prohibits companies within the European Union from direct or indirect (via subsidiaries or intermediary persons) compliance with the laws listed in the US Sanctions Annex. It also does not recognise any verdicts by courts that enforce US penalties. Reuters described the Blocking Statute more 'as a political weapon than a regulation', as its rules are 'vague and difficult to enforce'.

Otherwise, the term 'blocking statute' is not part of Austria's legal system. Of course, in cross-border cases, complying with a notice or subpoena in one country may often have implications in other countries. For example, a potential waiver of privilege is an important negative side-effect to consider. We have seen Austrian authorities accept well-argued excuses arising out of restrictions provided by foreign law, such as the potential waiver of privilege.

There is no blocking statute in Austria. However, the applicable data protection law, including the GDPR, must be considered in this regard, as it contains several requirements in connection with the cross-border transfer of data (see questions 21 to 23).

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Voluntary production of evidence may expose the management and board members who authorised the disclosure to liability, whereas compelled production entails no exposure to any liability.

As discussed in question 58, third parties with a duly substantiated legal interest may access the file of criminal proceedings, unless conflicting private or public interests prevail (section 77, StPO). Confidentiality therefore only extends to persons who lack a legal interest. The general public may gain knowledge of information contained in the file through the media. The accused, the defence lawyer, victims and third parties entitled to access the file are subject to regulatory restrictions (section 54, StPO) when passing on information obtained from the criminal file, in particular, when passing it on to the media. The media must take due account of the presumption of innocence when using the evidence and respect data protection laws (see question 60). Officials are under a duty of confidentiality (see question 58).

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Pursuant to the VbVG, corporations are subject to fines, which are measured in units per day, and to court directives (e.g., to compensate for harm done or to implement a proper compliance system). The current maximum fine for companies is €1.8 million (depending on the corporation's earnings). Moreover, they can be ordered to make redress, most notably in the form of compensation for harm done and donations to charity. The corporation cannot be indemnified by directors, officers or employees for fines imposed against the corporation (section 11, VbVG). However, the company may pursue its representatives for damages arising from a breach of their employment duties.

Natural persons are subject to the whole set of penalties and other sanctions if they are found (personally) guilty of an offence (section 18 et seq., StGB).

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Pursuant to the Federal Law on Public Tenders 2018 (BVergG), a company can be excluded from public tenders if one or more of its managers are convicted of an offence that casts doubt on the professional reliability of any of the managers. Companies participating in a public tender must provide proof of professional reliability by submitting criminal records issued by their home country (section 82(2), BVergG). However, a company may establish that, notwithstanding such a reason for exclusion, its professional reliability is guaranteed, notably by implementing measures preventing future offences.

64 What do the authorities in your country take into account when fixing penalties?

Section 5 of the VbVG contains a non-exhaustive list of aggravating and mitigating factors. Aggravating factors include gravity of harm done by a corporation, benefit flowing from the offence for the corporation, and toleration or facilitation of misconduct by employees. Mitigating factors include preventive measures taken by a corporation prior to the offence, including directives to adhere to the law issued to the employees, the employees being solely responsible for the offence, the contribution to the resolution of the case, compensation of harm done, essential measures to prevent future offences, and significant economic detriment to the corporation. The sentencing of natural persons follows similar principles (section 32, StGB).

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Non-prosecution agreements are not available in Austria. For the dropping of charges through diversion and closure of proceedings pursuant to section 18 of the VbVG, see question 51. The closure of a criminal prosecution by diversion has the advantage that the corporation is not condemned and no entry is made in the criminal register for corporations. The amount paid as a fine is also less than a fine imposed following a conviction for the same offence.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Law enforcement authorities have a duty to confidentiality (see question 58). For the possibility of limiting disclosure of information of the case files, see question 42.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Austrian law does not allow for settlements with law enforcement authorities. Under very limited terms, it is possible to resolve criminal prosecution by diversion (see question 51) or to benefit from the crown witness regulation (see question 28).

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

As far as publicly known, Austrian law enforcement authorities have not yet used external corporate compliance monitors as an enforcement tool.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Under Austrian law, private parties may declare a joinder of their civil claims to the criminal proceedings (section 67, StPO). Private plaintiffs who make a joinder declaration may access the criminal file insofar as their interests are affected (section 68, StPO).

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Investigations are not public in Austria (section 12, StPO). If a matter is deemed to be in the public interest, the prosecutor is asked to inform the public about the status of an investigation through the media offices of the larger courts and the public prosecutors. The co-operation of the prosecution authorities and courts with the media is governed by the Media Decree of the Federal Ministry of Justice JMZ 4410/9-Pr 1/2003, dated 12 November 2003.

Main trial and appeal proceedings are in the public domain (section 12, StPO), but may neither be broadcast on the radio or television, nor recorded by audio or visual means (section 228(4), StPO). In cases of public interest, it is common to have online live news ticker reporting. There are some exceptions to the principle of the public nature of a trial, including for reasons of public policy or to safeguard legitimate interests of the accused, witnesses or third parties.

However, a criminal file is accessible only to the accused and his or her defence lawyer, victims, private plaintiffs, and parties with a duly substantiated legal interest (section 77, StPO; see questions 61 and 69).

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common to use public relations (PR) firms. The author strongly recommends using firms that specialise in litigation PR and crisis management.

72 How is publicity managed when there are ongoing related proceedings?

The PR strategy should not only focus on managing the criminal trial, but also include all aspects of the legal matter, including (potential) civil liability matters.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Pursuant to section 155 of the BoerseG in conjunction with Regulation (EU) No. 596/2014 (the Market Abuse Regulation), companies publicly listed at the Vienna Stock Exchange must issue ad hoc notifications regarding inside information, namely information that has not been made public and, if it were made public, would be likely to have a significant effect on the price of the company's shares or other related financial instrument. Under certain circumstances, immediate disclosure can be delayed, in particular if it would impair the company's interests, the public is not misled and the fact that a settlement has been reached can be kept confidential to the point of its intended disclosure (see Article 17(1), Market Abuse Regulation).

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Currently, we are unaware of any specific projects to further address corporate misconduct.

8

Brazil

Heloísa Barroso Uelze, Felipe Noronha Ferenzini and João Augusto Gameiro[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Operation Car Wash is the largest corruption and money-laundering investigation in Brazil. There has been series of developments since the operation was launched in March 2014. It led to the indictment and imprisonment of key political figures in Brazil, such as former president Luiz Inácio Lula da Silva, and well-known businesspersons. Moreover, the operation has been divided into additional cases, including *Operation Resonance*, *Operation Fratura Exposta*, *Greenfield* and others.

2 Outline the legal framework for corporate liability in your country.

In Brazil, criminal liability is personal and subjective, which means that only individuals who have some degree of involvement in a criminal activity may be held liable for it.

In the vast majority of cases, legal entities, such as corporations or other non-natural persons, cannot be charged with crimes, but only for administrative and civil sanctions. The exception to this general rule is criminal liability for environmental crimes.

1 Heloísa Barroso Uelze, Felipe Noronha Ferenzini and João Augusto Gameiro are partners at Trench Rossi Watanabe. The authors wish to acknowledge the assistance of senior associate Silvia Helena Cavalcante de Almeida and associate Bianca Bonugli de Lima Amancio, Marcelo Ramos Leite, Natalie Ribeiro Pletsch, Tiago Caruso Torres and Gustavo Lima Kroger.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

In case of violations of the Anti-Corruption Law (Federal Law No. 12,846/2013), the highest authority of the relevant agency or entity of the executive, legislative and judiciary branches may investigate the matter and impose administrative sanctions. The Office of the Federal Comptroller General (CGU) has authority to investigate, process and sanction illegal acts set forth in the law that are committed against foreign public administration. At the federal executive level, the CGU will also have concurrent authorisation to initiate administrative proceedings against legal entities as well as to audit the proceedings handled by other authorities. In the case of judicial sanctions, prosecutors follow the procedure established by the Brazilian Class Action Law set forth in Law No. 7,347/1985.

Other authorities have power to enforce rules relating to specific legal areas, such as the Administrative Council for Economic Defence, which enforces antitrust violations, and the Securities Commission, which enforces rules relating to publicly traded corporations.

The Federal Court of Accounts has powers to review public disbursement and violations of public procurement laws.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The authorities must be aware of minimum elements of the occurrence of a crime to initiate an investigation. This means that a mere suspicion would not allow authorities to trigger an investigation; however, it is not necessary to have certainty about the occurrence of a crime or about the individuals responsible for it.

According to a Brazilian Supreme Court precedent, no criminal investigation can be initiated based only on anonymous information.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Individuals and legal entities may challenge the lawfulness or scope of a notice or subpoena from a law enforcement authority in the courts. Depending on the matter, individuals and entities may file a habeas corpus or an injunction.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Individuals can enter into a plea agreement with local authorities in exchange for a reduction in sentencing. Note that the agreement is usually signed by a federal or state prosecutor and only imposes the reduction.

7 What are the top priorities for your country's law enforcement authorities?

Corruption is the main object of the most recent and ongoing investigations in Brazil, which include *Operation Car Wash*, *Operation Resonance*, *Operation Fratura Exposta*, *Weak Flesh*,

Greenfield and others. *Operation Zelotes* is looking into bribery payments to tax authorities and politicians, in addition to an ongoing tax evasion investigation.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Brazil has no specific regulation on cybersecurity, but has approved a data privacy law that will enter into force in 2020. Certain violations, including distributing private photos, may be investigated and prosecuted by local authorities.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Brazilian law includes specific norms against cybercrime activities (e.g., hacking of devices and illegal wiretapping). Also, other norms may apply to illegal activities conducted via the internet, software or hardware (e.g., terrorism, crimes against intellectual property of computer software, crimes against children and teenagers, crimes against honour, racism and xenophobia).

As a rule, cybercrimes are investigated by the Brazilian state police departments. However, the Federal Police is specifically allowed to investigate (1) terrorism crimes, (2) crimes involving misogynistic crimes, or internet activity that amounts to hatred or aversion of women and (3) crimes that have a transnational characteristic, all of which Brazil is committed (via international treaties) to combat and prevent.

In general, the state police departments, Federal Police and public prosecutors' offices will have specialist teams in charge of the criminal investigation and prosecution of cybercrime and wrongdoing committed via the internet, software and hardware. Police departments, public prosecutors' offices and court teams work round the clock and are available for considering and deciding emergency criminal cases.

Brazil has entered into multilateral and mutual legal assistance treaties with various countries, which set forth proceedings and include provisions for dawn raids, freezing of assets, interviews, delivery of documents, etc. to obtain information or documents to be used in a criminal investigation or lawsuit, including any relating to cybercrime.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

The Criminal Code sets forth the requirements for applying Brazilian criminal law to crimes that have occurred abroad (from start to finish) (Articles 7 and 8, Criminal Code). Brazilian jurisdiction has extraterritorial effect in two sets of possible situations. The first of these is the consideration of genocide (when the offender is Brazilian or is living in Brazil) and crimes committed against:

- the Brazilian president's life or freedom;
- public trust;

- property owned by public administrative bodies;
- companies owned by public administrative bodies or public foundations; or
- a public administrative body, including crimes against an individual who is acting on behalf, or under the orders, of a public administrative body.

An offender who commits any of the above-mentioned crimes should be punished according to Brazilian criminal law even if he or she has been acquitted or convicted by a foreign court.

The second series of situations require different conditions to be applied according to the type of crime, including crimes that Brazil is obliged to repress based on an international treaty or convention, or those committed by Brazilian individuals or in Brazilian aircraft or vessels (commercial or private) in a foreign territory if no other court decision on its merits has been issued.

In addition, for Brazilian jurisdiction to be applied, all the following conditions should be fulfilled:

- the offender must be in Brazil for criminal prosecution to begin, and must:
  - not have been previously acquitted by a foreign court or fully served a penalty abroad;
  - not have been acquitted or pardoned by a foreign court; and
  - be criminally liable (e.g., the statute of limitation was not reached);
- the fact must be deemed a crime under the criminal law of both countries; and
- Brazilian law must authorise extradition in such a case, if required.

If a Brazilian citizen is the victim of a foreign individual's conduct, Brazilian jurisdiction is applied provided that (1) the above-mentioned conditions are fulfilled, (2) extradition of the offender has not previously been requested or denied, and (3) the Brazilian Minister of Justice has requested the law enforcement authorities to punish the crime.

Note that the hypothesis of jurisdictional extraterritorial effects is related to crimes that occurred abroad (from start to finish). Indeed, if any part of an individual's action or omission essential to the occurrence of a crime has taken place in Brazil, Brazilian Criminal Law determines that the crime was committed in Brazil. Also, if an individual's action or omission essential to the occurrence of a crime has taken place abroad, but its result occurs in Brazil, again the crime is considered as having been committed in Brazil. Consequently, both hypotheses (action/omission and its results in Brazil) would be under Brazilian jurisdiction. This means none of the conditions relating to the extraterritorial effects, as described above, needs to be complied with for the offender potentially to be criminally charged in Brazil.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Brazilian authorities both co-operates on criminal matters with foreign authorities and requests the co-operation of foreign authorities. Co-operation between authorities can involve the execution of acts relating to the collection of evidence (interviews, breach of bank secrecy), transfers of convicted individuals, freezing of assets, etc., during criminal investigations or lawsuits. Brazil has multilateral and bilateral co-operation agreements with various countries. If there is no previous agreement between the countries, it is possible to enter into a mutual commitment for future situations.

The main challenges faced in cross-border investigations are (1) the time spent waiting for other countries' answers or proceedings, (2) the necessary observation of formalities to ensure that the evidence collected abroad would be considered valid in Brazil (not null or illicit), and (3) situations in which Brazil does not have a previous agreement.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

As a general rule, double jeopardy is not allowed according to Brazilian law.

Exceptions apply regarding the extraterritorial effects of genocide (when the offender is Brazilian or is living in Brazil) and crimes against (1) the Brazilian president's life or freedom, (2) public trust or property owned by public administrative bodies, or companies owned by public administrative bodies or public foundations, (3) public administrative bodies, including crimes against an individual who is acting on behalf of an administrative body (see question 10).

However, those hypotheses do not relate to crimes against the environment, which are the only crimes for which legal entities are potentially criminally liable in Brazil (see question 2).

13 Are 'global' settlements common in your country? What are the practical considerations?

Brazilian legislation has no clear disposition regarding global settlements, including the possibility and requirements. Nevertheless, a higher number of global settlements have involved Brazilian companies (e.g., Embraer, Petrobras, Odebrecht/Braskem).

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Although Brazilian authorities should conduct their own investigations, it is common for the essential evidence to be collected to ensure a conviction relying on co-operation agreements with foreign authorities investigating similar matters. Moreover, the Criminal Code provides that, and respecting foreign judicial decisions, when the application of Brazilian law would produce the same consequences and civil remedies, such as damages orders and restitution, or other security measures, can be recognised and enforced in Brazil if the necessary requirements are fulfilled.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

The Brazilian Clean Company Act, issued in 2013, may require financial penalties to be imposed on companies involved in corrupt acts, which can amount to as much as 20 per cent

of the gross revenue in the year prior to commencement of the administrative sanctioning proceeding, plus loss of assets representing the undue advantage obtained. Other Brazilian legislation may regulate similar irregularities and lead to companies facing debarment from entering into contracts with the government.

In terms of economic sanctions, the Head Minister of the CGU has signed 11 leniency agreements involving the payment by sanctioned companies of more than 11 billion reais to the Treasury (including fines and reimbursement of damages). Also, at the federal level, Brazilian authorities have, to date, barred more than 12,000 companies from entering into contracts with public administration authorities.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

The level of enforcement action has increased dramatically during the past decade. In the past, executives of large companies and politicians were rarely arrested. Currently, based only on the Federal Public Prosecutor's website regarding *Operation Car Wash* in Paraná (updated in July 2019), almost 2,500 proceedings have been conducted, including 1,237 search and seizure warrants, more than 300 arrests and 11 leniency agreements.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Brazil has signed several co-operation agreements with enforcement agencies in countries such as Chile, Switzerland and the United States.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Brazil has not enacted any blocking legislation.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct most often come to the attention of companies through whistle-blowers, either in-house or external, investigations conducted by enforcement authorities and internal audits (often with the assistance of external auditors).

Information gathering

21 Does your country have a data protection regime?

Brazil has passed data protection legislation that will enter into force in 2020. The law will limit access to an individual's personal data.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

It is still uncertain how the data protection regime will be enforced. The Data Protection Authority was created only in July 2019, and no directors have been appointed yet. It is therefore not yet clear whether the main purpose of the Data Protection Authority will be to educate society in general or to impose sanctions.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

The new data privacy law may generate discussions about data collection and access to employees' personal information during an internal investigation.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

No. Under the current system, accessing employees' communications on corporate devices is permitted.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Yes. Recent major criminal investigations (e.g., *Mensalão*, *Car Wash*, *Zelotes* and *Greenfield*) show that search warrants and dawn raids have been the mechanism for public authorities to collect evidence more quickly and effectively. Under Brazilian criminal law, the police must present a specific search and seizure warrant, duly authorised by the court, for a particular department of the company or for material pertaining to certain employees. General searches inside company premises are not allowed. If authorities exceed the limits of the search warrant, both the individuals and companies involved and affected by the improper collection of evidence can claim for such documents to be retracted and excluded from the case.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Under Brazilian law, attorney–client communication is privileged and confidential. The definition of specific spaces within the legal department and the explicit identification of

documents covered by privilege are ways to protect material from being improperly seized during a dawn raid.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Under Brazilian criminal law, individuals who are suspected of involvement in committing an offence cannot be compelled to give testimony. Such individuals also have the right against self-incrimination and there is no crime of perjury. Compelled testimonies regarding such individuals are illegal and cannot be used in criminal procedures.

Witnesses, on the other hand, are obliged to collaborate with an investigation. If witnesses do not comply with an order to attend a hearing, they can be sanctioned with a fine, can be coercively conducted to a police station or court, and be charged with the crime of disobedience.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Law 13608/2018 establishes that any individual may report a crime to public authorities and may have their identity protected. There is no financial incentive to whistleblowers in Brazil.

In the corporate world, the Clean Company Act regulates the requirements for a compliance programme, which should contain a proper whistleblower channel and policies regarding confidentiality and non-retaliation.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employment law in Brazil has undergone major changes, but it continues to be protective towards employees. As regards conduct within the scope of an investigation, it is recommended that an employee be allowed to defend their actions and counter any accusations.

The investigation must adhere to the required levels of secrecy and discretion to avoid anything being revealed that might cause harm to the employee.

There is no distinction between officers and directors.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

An employee involved in misconduct may be reprimanded or dismissed with cause. In either case, he or she has the right to apply for the matter to be addressed in court.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

No.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

This should be assessed on a case-by-case basis, taking into consideration the company and the complexity of the investigation to be undertaken. However, in general, it is deemed good practice to prepare a document that sets out a list of the matters that need to be clarified by the investigation and which mechanisms will be used to achieve those clarifications (e.g. gathering computer records and mobile phone data, interviews and background checks), such as identifying the parties potentially involved in the alleged irregularities, any violations of the relevant legislation and which authority has jurisdiction in the matter.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

In the first instance, is it recommended that, according to Brazilian labour laws, any individuals who may be involved in an offence be suspended. Second, companies must make sure that they collect as much evidence as possible relating to the offence, as this can be used in the company's defence (if a charge is brought) or to conclude a leniency agreement (as it will require the company to provide clear evidence of the misconduct and to help identify the individuals involved). In addition, the Brazilian Anti-Corruption Law includes provisions relating to interference with investigations and, therefore, the company must issue a retention notice to all employees warning that no documents or data should be eliminated until further notice.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

If a company receives a subpoena, it should immediately involve its legal team (in-house, external or both) to identify the extent of the allegations, the potential risks, whether other authorities would also have jurisdiction, and which stakeholders should be informed.

The company must respond to the relevant authority in a timely manner, be co-operative, transparent and provide all the information requested, in an accessible format. It is also very important to establish which documents are subject to the attorney–client privilege and that they be dealt with accordingly.

The company should also evaluate and indicate which information and documents should be treated by the authorities as confidential, such as trade secrets.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

The timing and quality of disclosure should be considered in each case or event. Therefore, the decision to publicly report the existence of an internal investigation or contact by law enforcement depends on several factors, including whether the company has shares that are publicly traded.

36 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are currently encouraged by local law enforcement agencies and, in some cases, local authorities request the assistance of internal investigators to structure their cases.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Any communication between an attorney and a client in the context of a representation are protected in Brazil and are not subject to disclosure to third parties, with limited exceptions. Considering this main rule, an internal investigation may claim privilege over any investigative act conducted under the direction of a lawyer duly registered with the Brazilian Bar Association. To safeguard the protection of privilege, the involvement of individuals who are not lawyers must be as limited as possible.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Under the Brazilian legal system, privilege rules protect any communication between a lawyer and a client in the context of legal representation. The Brazilian Bar Association Code of Ethics provides that an attorney has a duty to maintain confidentiality of all facts of which he or she has become aware while practising law, including activities of mediation, conciliation and arbitration. The rule makes no distinction between a company or an individual.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The attorney-client privilege protects communications involving lawyers and makes no distinction between in-house or external lawyers. To claim such privilege, the lawyer must be licensed by the Brazilian Bar Association and must have received a power of attorney from the client (individual or company) that is being represented.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

If the legal advice was provided by a lawyer licensed and registered at a foreign bar association and the advice was requested under the direction of a Brazilian lawyer, the advice is protected by Brazilian legislation.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Waiver of the attorney–client privilege may be requested by authorities as part of a plea agreement or a leniency agreement. Usually, at the beginning of settlement discussions, the authorities and the individual or company sign a non-disclosure agreement to protect the information that will be shared in the context of the negotiation. After the agreement is signed, a waiver may be included in the resolution.

The attorney–client privilege may be waived in other circumstances, including at the client's request, and may be breached if the communication is in furtherance of a crime, if it may avoid a threat to someone's life or honour, or if an attorney needs the information for his or her own protection or in defence of the client.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

There is no specific regulation covering the extension of a waiver or the prohibition of a limited waiver. In this context, the client may claim a limited waiver. Note that legal proceedings in Brazil have a different level of secrecy and, in some instances, the docket case file may be deemed entirely confidential at the court's discretion.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

As discussed in question 42, clients may claim limited waiver in Brazil and thus privilege may be claimed over information provided from another country.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Parties with a common interest may share privileged information in Brazil as long as lawyers duly represent them and they have authorised communication between counsel.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Considering that the attorney–client privilege in Brazil requires the directive involvement of a lawyer, it is not clear whether the protection may be extended to other parties and must therefore be considered on a case-by-case basis.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Yes. Provided an attorney was involved in the process, privilege may be claimed.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Brazilian legislation has no provision in this regard. Nevertheless, it is deemed advisable to indicate that the content of the interview is privileged and that the witness should regard the matter as confidential.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Typically, the lawyer conducting the investigation should have a list of questions and documents to be shown as evidence to a witness. Employees, if they so wish and at their request, may have their own legal representation at the interview.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Reporting misconduct is not mandatory in Brazil. However, if a company or individual wants to enter into a leniency agreement or plea agreement, co-operation is required.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting is advisable when a company wants to enter into a leniency agreement to obtain the benefits of self-reporting and co-operation.

Prior to self-reporting, it is highly recommended to identify which authorities are likely to have jurisdiction over the matter and contact them all, to mitigate any risk of legal uncertainty in connection with a subsequent investigation and to avoid any lawsuits being initiated by other authorities on the basis of the information reported to a specific authority.

This same process should be extended to foreign countries. If other potential jurisdictions are identified, it is recommended to seek legal advice in those countries to establish whether self-reporting is advisable, and to aim to reach a global settlement.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

Self-reporting can be very complex in Brazil as more than one enforcement agency may have an interest in any single case. For example, based on the Clean Company Act, the federal comptroller general, the Federal Prosecutor's Office and the Office of the Attorney General should participate in a leniency agreement.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

In cases where a company has already launched an internal investigation and may be expecting contact from the relevant authorities, the counsel conducting the investigation should recommend the best strategy. When a notice or subpoena is issued unexpectedly, the company should immediately retain an experienced counsel and discuss the best approach.

Some authorities are open to being approached by companies and may agree to initiate discussions on a possible settlement. Other authorities are more restricted and may not agree to provide any information to companies. In the latter case, companies may claim access to investigative proceedings in court.

54 Are ongoing authority investigations subject to challenge before the courts?

Any individual or company under investigation may challenge proceedings in a court of law if any rights are violated. The challenge may be broad, such as to terminate the investigation, or limited, with respect to a specific act or piece of evidence.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Based on recent cases in Brazil, it is clear that Brazilian and foreign authorities are in constant communication and have shared relevant information between them. Thus, it would be advisable to retain counsel in all countries that may be involved in the enforcement actions. Counsel should decide the best strategy on a case-by-case basis and, if possible, should initiate communications with all authorities at the same time.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In general, a company must search and produce any material requested by the authorities. It is important to note that, if the material or documents are located in a country with restricted privacy laws, the company must retain local counsel and must report the legal conflict to

the authorities. In certain cases, to avoid local claims, the foreign authorities should request production of the document directly to a local authority and not to the company.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

As has been seen during the *Operation Car Wash* investigations, the Brazilian authorities have shared and received information from several authorities, including in the United States and Switzerland. Brazil has signed bilateral co-operation agreements with several other countries, including Chile and Switzerland, and has ratified international agreements such as the Palermo Protocols and the US Foreign Account Tax Compliance Act.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

The Supreme Federal Court is expected to deliver a final decision (by the end of 2019) regarding the legality and extent of the sharing of information obtained by financial intelligence units with prosecutors, and whether prior authorisation from a judge is necessary. That decision will be a key factor in current and future investigations.

As regards the content of a leniency agreement, its provisions will regulate restrictions on the sharing of information. There are court precedents authorising the sharing of information with other authorities, provided that the restrictions agreed by the parties are respected.

Any evidence gathered during the course of investigations conducted by prosecutors shall be confidential, and withheld from any third parties.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Some authorities have a duty to preserve the confidentiality of investigation proceedings (such as the police and the Council for the Control of Financial Activities). However, they must share any information that relates to criminal activities or felonies with other authorities who have launched criminal proceedings. A docket criminal case may be deemed to be sealed (to protect a victim or if the victim is a minor), but the main ruling deems that any criminal case should be public and accessible. Companies may claim secrecy, but the matter will be decided by the judge responsible for the case.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Brazil has just promulgated a data protection law that is expected to enter into force in 2020. According to this law, companies and individuals may only retain information about other individuals or companies if supported by particular requirements. It is not clear how the law will be implemented.

There is existing legislation that regulates international law and requires approval from the Superior Court of Justice for the enforcement of international decisions or subpoenas. Such decisions or subpoenas will not be deemed valid and enforceable if they violate Brazilian sovereignty.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

There is no particular risk for voluntary production. Considering that co-operation may result in a reduction of sanctions in the context of the Brazilian Anticorruption Law, companies may consider voluntary disclosure. Once produced (voluntarily or compelled), the material may be discoverable if there is no requirement to maintain secrecy in the case. There is no particular confidentiality in the production of material, but a company may request secrecy in respect of all material or business-related information.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Following conviction, penalties that may be applied to individuals (including company directors) are imprisonment, restriction of rights, or fines.

The restriction of rights may be substituted for imprisonment if the following requirements are fulfilled: (1) the penalty applied is less than four years' imprisonment and no violence or serious threat was used (in case of negligent conduct, there is no temporal limit); (2) the convicted person should not have committed the same wilful crime previously (specific recidivism prevents this substitution); and (3) the offender's personal characteristics and behaviour should indicate that such penalties are adequate.

According to the Criminal Code, restriction of rights can include:

- payment to the victim or to charitable entities;
- confiscation of assets and valuables;
- attending conferences or courses, or participating in educational activity at a prison facility, for five hours on a Saturday and Sunday;
- community service;
- temporary removal of certain rights, such as holding a public or elective position, joining a profession that requires a special licence or authorisation from public agencies, visiting certain locations, or applying for public competitions, evaluations or exams.

Other types of restriction of rights penalties can be applied in specific instances, such as for crimes against consumers (under Federal Law No. 8,078/1990) or environmental crimes (under Federal Law No. 9,605/1998).

Legal entities are subject to the following criminal penalties:

- fine;
- community service;

- partial or total suspension of activities;
- temporary restrictions on establishments, plants, projects or activities;
- disqualification from contracting with government entities, and from obtaining public subsidies, grants or donations for up to 10 years (Article 22, Federal Law No. 9,605/1998).

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

From a criminal perspective, settlement in another country does not prevent a company (or its directors) being held criminally liable in Brazil. In view of the co-operation between authorities, information presented to a foreign authority can potentially be shared with Brazilian authorities and, therefore, expose the company and its directors to criminal liability in Brazil.

64 What do the authorities in your country take into account when fixing penalties?

Brazilian courts should follow three steps to determine the penalties that will be imposed on an individual. In the first instance, the court should consider:

- regarding the individual: his or her culpability, criminal background and social behaviour;
- regarding the crime: the motivations, circumstances and consequences; and
- regarding the victim: his or her conduct (i.e., any contribution to, or facilitation of, the crime).

Second, penalties should be made more severe in consideration of:

- recidivism by the offender;
- the motivation for the crime;
- how the crime was committed;
- who the victim is;
- the behaviour of the offender during the crime;
- the context in which the crime was committed; and
- the leadership of the offender.

Conversely, penalties may be reduced in consideration of:

- confession of the crime by the offender;
- the offender's age;
- the motivation for the crime; and
- any attempt by the offender to mitigate the consequences of the crime.

As a third step, the court should consider general or specific criteria – depending on the crime in question – to increase or decrease penalties (e.g., attempted use of a firearm).

In relation to fines, criminal law prescribes certain parameters. In addition, the financial situation of the offender should be considered in applying an appropriate penalty.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

No. However, Brazil has settlements in place to mitigate sanctions in the form of leniency agreements.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Reporting restrictions or anonymity for corporates are determined in each leniency agreement to ensure the effectiveness of the collaboration and the useful outcome of the lawsuit. In general, to ensure fairness in these proceedings, a proposed leniency agreement will not be announced to the public until after the agreement is effective or after the district attorney's office presses charges against the defendants.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Companies must understand that a settlement must be negotiated with all the enforcement agencies at the same time.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

There is no legal provision regulating the use of external monitors, although there has started to be some use of this tool in Brazil, such as in the *Odebrecht* case.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Third parties may file an indemnity or contractual judicial claim and a court or authority may decide to provide access to third parties.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

According to Brazil's Criminal Procedure Law, a police investigation is generally public. However, an investigation may be conducted in secret when this measure is necessary for the police to ensure the effectiveness of the investigation or to protect the identity of a suspect or victim. Individuals under investigation and their attorneys are entitled to have access to the records of the investigation, except any measures that are still being conducted (e.g., searches and seizures that are still being prepared or ongoing wiretapping).

Criminal lawsuits are also public, unless secrecy is necessary to protect the privacy and identity of the defendant or the victim.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common for larger companies to use external public relations companies, and publicly traded companies make use of their internal investor relations departments. These are the most common options for handling external communications. In view of the vast repercussions from involvement of the media in Brazilian corruption cases, it is suggested that companies seek the assistance of consultants who specialise in investor relations (if the company is listed) or a public relations firm that specialises in crisis management. It is also recommended that companies put in place internal procedures for handling these kinds of situations.

72 How is publicity managed when there are ongoing related proceedings?

Companies should always be aware of the pros and cons of disclosing, or not disclosing, relevant information in relation to an ongoing investigation. Furthermore, it is advisable that the attorneys responsible for the case always be involved in the decision-making process to avoid a higher degree of risk regarding the individual's or company's liability.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

This should be assessed on a case-by-case basis, but is mainly dependent on whether the matter involves a publicly traded company, in which case, the company has a duty to disclose material information regarding the its business and finances, as they relate to the settlement.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

The data privacy law is due to enter into force and will restrict access to certain information. This may have a great effect on internal investigations and on the sharing of information with the authorities. Further, several bills of law are in Congress, which may have a great effect on anti-corruption measures. One of the proposals is to impose limits on certain investigation measures and to make any wrongdoing or misconduct by a member of the judicial or police authorities a criminal offence. Finally, a new anti-corruption project put forward by Minister of Justice Sérgio Moro is under discussion in Congress.

9

Canada

Graeme Hamilton and Milos Barutciski[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

In February 2015, the Royal Canadian Mounted Police (RCMP) charged leading Canadian construction and engineering company SNC-Lavalin Group Inc in connection with alleged fraud relating to the construction of a Montreal hospital and alleged bribery of foreign officials in Libya. Following the initiation of the investigation, the company replaced its senior management and board and introduced robust compliance policies and procedures. SNC-Lavalin pleaded not guilty to the charges and, in May 2019, a judge of the Court of Quebec in Montreal determined that the Crown had met the evidentiary burden to commit the company to trial. The case is widely expected to set an important benchmark for corporate criminal liability in Canada.

It was expected by many observers of the matter that the recent enactment of amendments to the Criminal Code introducing deferred prosecution agreements in Canada (known as remediation agreements) would lead to a possible negotiated settlement of the charges. However, the company was informed by the Director of the Public Prosecution Service of Canada in early October 2018 that the prosecution was not prepared at that time to initiate negotiations for a remediation agreement.

In February 2019, a national newspaper in Canada reported that the Prime Minister's Office had placed improper pressure on the then-Attorney General to intervene in the prosecution so that SNC-Lavalin could secure a remediation agreement. Shortly after the decision

1 Graeme Hamilton and Milos Barutciski are partners at Borden Ladner Gervais LLP. The authors would like to thank their associates, Alannah Fotheringham, Omar Madhany and Julia Webster, for their assistance with this chapter.

to not offer SNC-Lavalin a remediation agreement, the Attorney General was transferred to the Ministry of Veterans Affairs as part of a cabinet shuffle. Although the Prime Minister's Office disputed the newspaper report, the former Attorney General resigned from cabinet and spoke out against the Prime Minister's Office during testimony before a House of Commons committee. The Prime Minister eventually expelled the former Attorney General from the Liberal caucus in April 2019 and the matter was front-page news in Canada for several weeks.

2 Outline the legal framework for corporate liability in your country.

Criminal law applies broadly to 'organisations', including corporations and partnerships. The liability of a corporation is assessed through an evaluation of the actions of its senior officers. 'Senior officers' are defined to include a representative who plays an important part in the establishment of an organisation's activities and, in the case of a body corporate, includes a director, its chief executive officer and its chief financial officer. A 'representative' is defined as a director, partner, employee, member, agent or contractor of the organisation.

For offences that require the prosecution to prove fault (apart from negligence), a corporation will be a party to an offence, if, with the intent at least in part to benefit the organisation, one of its senior officers (1) acting within the scope of his or her authority, is a party to the offence, (2) having the mental state required to be a party to the offence and acting within the scope of their authority, directs the work of other representatives of the organisation so that they carry out the act or make the omission specified in the offence, or (3) knowing that a representative of the organisation is or is about to be a party to the offence, does not take all reasonable measures to stop them from being a party to the offence.

For offences that require the prosecution to prove negligence, an organisation is a party to an offence if (1) one of the organisation's representatives, acting within the scope of his or her authority, is a party to the offence, and (2) the senior officer responsible for the aspect of the organisation's activities relevant to the offence departs markedly from the standard of care that could reasonably be expected to prevent a representative of the organisation from being a party to the offence.

In addition, there are a multitude of provincial and federal strict and absolute liability offences for which a corporation can be prosecuted but that do not require proof of intent.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The law enforcement authorities most frequently encountered by corporations are the Canadian Competition Bureau (which enforces the Competition Act), the RCMP (which typically investigates alleged breaches of the Corruption of Foreign Public Officials Act as well as complex, multi-jurisdictional terrorist financing and money laundering offences proscribed by the Criminal Code) and the provincial securities regulators (which enforce provincial securities legislation). There are no specific policies pertaining to the prosecution of corporations.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

No particular threshold of suspicion is required. However, to take investigative steps that involve compelling the production of documents from the target of the investigation or third parties, the authorities generally need reasonable grounds to believe that an offence has been committed. The one exception is securities regulatory investigations, for which there is no threshold of suspicion necessary for provincial securities regulators to issue a summons.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Subpoenas are generally not a tool that is available to law enforcement authorities at the investigative stage. There is no way to compel individuals to provide statements, and documents can only be obtained from the target of an investigation through a search warrant. The one exception is securities regulatory investigations, for which provincial securities regulators do have the authority to compel individuals to be interviewed by way of a summons and to compel the production of documents.

A summons from a provincial securities regulator can be challenged through an application to a court to quash the summons. However, such an application would generally need to be premised on a challenge to the regulator's jurisdiction to issue the summons.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Immunity agreements for individuals who co-operate with authorities are available. They generally involve an agreement by the Crown to refrain from prosecution or to terminate a prosecution regarding an individual in exchange for that individual's co-operation. The Crown will typically offer an immunity agreement when the individual's co-operation is of significant value such that it is clearly in the public interest not to hold the individual accountable for criminal activity. In making this determination, the Crown will examine a variety of factors, including:

- the seriousness of the offence at issue;
- the reliability of the individual;
- the reliability of the anticipated evidence;
- the importance of the individual's co-operation;
- the nature and extent of the individual's involvement in the offence at issue; and
- protection of the public.

When the Crown determines that an immunity agreement is not warranted, an individual may still receive leniency as a result of co-operating with the authorities. Co-operation with the authorities is a well-recognised mitigating factor during sentencing and so sentencing judges will regularly take co-operation into account when imposing a sentence on an accused. Section 3.3 of the Public Prosecution Service of Canada Deskbook provides guidance on immunity agreements and sets out the applicable criteria in determining whether the Crown should enter into an immunity agreement, discusses the handling of co-operating information

providers and distinguishes the role of the Crown from that of the investigating agency in the immunity process.

7 What are the top priorities for your country's law enforcement authorities?

Enforcement authority is divided by subject matter, level of government (federal, provincial or municipal) and geographical jurisdiction. As a result, enforcement priorities vary considerably across the country and by subject matter. In recent years, the RCMP has indicated that it is giving priority to organised crime, terrorism and national security and economic crimes. At the provincial level, priorities have varied, with money laundering attracting greater priority in British Columbia and corruption being a key focus in Quebec.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Cybersecurity is regulated through both federal and provincial legislation. At the federal level, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to federal government organisations and to businesses in provinces that do not have 'substantially similar' privacy protections. Under PIPEDA, covered organisations must protect personal information with security safeguards that are appropriate to the sensitivity of the information. The security safeguards must protect the information against loss or theft, as well as unauthorised access, disclosure, copying, use or modification. The Privacy Commissioner of Canada oversees compliance with PIPEDA.

Recent amendments to PIPEDA now require covered organisations to notify the Privacy Commissioner and affected individuals, as soon as is feasible, of breaches of security safeguards involving personal information under the organisation's control. Organisations are subject to this mandatory reporting regime if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to individuals. Organisations that knowingly fail to comply with these provisions are subject to criminal punishment.

The provinces of Alberta, British Columbia and Quebec have legislation in force that is substantially similar to PIPEDA and so businesses in those provinces are subject to provincial legislation.

In addition to federal and provincial legislation, various industry regulators, such as the Mutual Fund Dealers Association and the Investment Industry Regulatory Organization of Canada, also publish guidance documents that set expectations for how regulated entities are to address cybersecurity risk. Further, the Canadian Securities Administrators have notified registered firms in Staff Notice 33-321 (Cyber Security) that registered firms should ensure their compliance systems address the risks of cyber threats and cybersecurity.

In June 2019, Desjardins Group, a leading Canadian banking institution, reported a serious data breach in which the social insurance numbers, names, dates of birth and addresses of 2.7 million customers were compromised. As a result of the data breach, the bank is currently subject to a joint investigation by the Privacy Commissioner of Canada and the provincial privacy authority of Quebec into whether it complied with applicable federal and provincial privacy laws. The Privacy Commissioner of Canada has conducted

similar investigations into past data breaches at Equifax Inc in 2017 and VTech Holdings Ltd in 2015, which resulted in findings that both organisations failed to implement adequate security safeguards.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The Criminal Code contains a wide variety of offences that authorities in Canada have historically used to combat cybercrime. The RCMP, which is generally responsible for combating large-scale cybercrime in Canada, distinguishes between cybercrime that involves technology as a target and cybercrime that involves technology as an instrument. In the former category, the RCMP includes criminal offences that target computers or other information technologies, such unauthorised use of a computer and mischief in relation to computer data. In the latter category, the RCMP includes criminal offices that are committed using the internet and information technology, such as fraud, identity theft, intellectual property infringements and money laundering.

In addition to the RCMP, cybercrime offences may be investigated by other relevant federal government agencies and local police authorities across the country. The RCMP typically works in partnership with these other authorities to investigate cybercrime issues that fall within overlapping jurisdictions. For example, the Canadian Anti-Fraud Centre is a combined effort by the RCMP, the Ontario Provincial Police and Competition Bureau of Canada to counter internet and mass-marketing fraud.

In February 2018, the federal government announced the creation of the National Cyber Crime Co-ordination Unit, which aims to coordinate cybercrime investigations across Canada, provide a single national reporting mechanism for incidents of cybercrime and work with Canada's global partners to combat cybercrime. In that regard, Canada has ratified the Council of Europe's Convention on Cybercrime (also known as the Budapest Convention) and actively participates in international efforts to combat cybercrime, such as the Inter-American Cooperation Portal on Cyber-Crime.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In general, Canadian criminal law does not apply extraterritorially. Section 6(2) of the Criminal Code provides that 'no person shall be convicted . . . of an offence committed outside Canada' unless a specific provision provides otherwise. That said, 'outside Canada' has been judicially interpreted in the leading Supreme Court of Canada case (*R v. Libman*) as lacking a 'real and substantial' connection to Canada. In other words, an offence committed outside the territory of Canada could be prosecuted in Canada if there remains some 'real and substantial' link to Canada.

Importantly for corporations, many relevant proscriptions contain language that gives them extraterritorial effect. For instance, both the anti-money laundering (AML) provision in the Criminal Code and the terrorism financing provision contain specific language to give them extraterritorial effect. The AML provision prohibits dealing in property acquired

as a result of the commission abroad of an act that would be a criminal offence in Canada. A terrorism financing offence is deemed to be committed in Canada when there is a nexus between the underlying terrorist act and Canada, either through the perpetrator or the victim, or if the person who commits the terrorist financing offence is linked to Canada. In addition, bribery of foreign officials in contravention of the Corruption of Foreign Public Officials Act is prosecutable in Canada if the offence is committed by a corporation, firm or partnership that is 'incorporated, formed or otherwise organised under the laws of Canada or a province'.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border criminal investigations are often hampered by difficulty in obtaining information from foreign sources. Canada has mutual legal assistance treaties (MLATs) with some 40 countries and Canadian legislation allows non-treaty assistance. MLAT requests can be time-consuming and administratively burdensome. Canadian authorities also have enforcement co-operation agreements and memoranda of understanding with counterpart agencies in other countries in matters such as competition law and securities. Informal co-operation also takes place between Canadian enforcement agencies and their foreign counterparts; however, the extent of co-operation is often limited as a result of statutory and policy restrictions on disclosure of confidential information.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Double jeopardy and similar principles apply in Canada to limit the criminal exposure of a defendant that has already been convicted in another jurisdiction of a relevant offence. To determine whether such principles apply, a Canadian court will typically assess whether the foreign offence and the Canadian offence at issue have a sufficiently close legal nexus (i.e., elements of the offences) and factual nexus (i.e., factual basis for the offences).

There is no analogous policy in Canada to the 'anti-piling on' policy that exists in the United States.

13 Are 'global' settlements common in your country? What are the practical considerations?

No.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Canadian enforcement authorities do not, as a general matter, defer to the findings of foreign agencies (absent a double jeopardy issue where the same matter has been definitively

determined by a foreign court). That said, Canadian authorities will consider both the fact of and the outcome of foreign investigations when determining priorities for case and resource allocation.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Canadian sanctions are imposed under five statues:

- the United Nations Act, whereby Canada implements sanctions mandated by the United Nations Security Council, which are consistent across UN Member States;
- the Special Economic Measures Act, whereby Canada maintains unilateral measures against certain foreign states in cases where a grave breach of international peace and security has resulted or will result in a serious international crisis, a foreign state commits gross and systematic human rights violations, a foreign state or foreign public official is responsible for or complicit in significant acts of corruption, or where an international body, of which Canada is a member (other than the United Nations), recommends for its members to enact economic measures against a foreign state;
- the Justice for Victims of Corrupt Foreign Officials Act, whereby Canada may impose measures against foreign nationals who are responsible for, or complicit in, gross violations of human rights or corruption;
- the Criminal Code, which enables Canada to sanction terrorist entities, including those not listed by the United Nations Al-Qaeda and Taliban Regulations or the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism; and
- the Freezing Assets of Corrupt Foreign Officials Act, which allows Canada to freeze the assets or restrain the assets of politically exposed foreign persons believed to have misappropriated or acquired property improperly.

Sanctions are implemented by the government in the form of statutory regulations. The measures imposed on specific states, organisations and individuals may take varying forms, such as arms and related material embargos, asset freezes, export and import restrictions, financial prohibitions and technical assistance prohibitions.

Canadian sanctions measures are in force against the following states: Central African Republic, Democratic Republic of the Congo, Eritrea, Iran, Iraq, Lebanon, Libya, Mali, Myanmar, Nicaragua, North Korea, Russia, Somalia, South Sudan, Sudan, Syria, Ukraine, Venezuela, Yemen and Zimbabwe. Schedule 1 of the Justice for Victims of Corrupt Foreign Officials Regulations lists all designated individuals, which include individuals from Russia, Venezuela, Myanmar, South Sudan and Saudi Arabia. Canada has enacted measures under the Freezing Assets of Corrupt Foreign Officials Act against Tunisia and the Ukraine.

Global Affairs Canada is generally responsible for the administration of Canadian sanctions and works with other agencies in enforcement matters (notably the RCMP and the Canada Border Security Agency).

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

There has been increased scrutiny of compliance with sanctions measures by Global Affairs Canada.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Yes, Global Affairs Canada co-operates with its counterparts in other countries to enforce Canadian sanctions measures.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Canada has enacted the Foreign Extraterritorial Measures Act (FEMA) in relation to the extra-territorial measures of foreign states. FEMA prevents Canadian individuals and companies from complying with foreign laws in Canada and authorises the Canadian federal cabinet to issue orders to block or otherwise counter the effects of foreign extraterritorial measures in Canada.

The only foreign extraterritorial law blocked under FEMA is the United States embargo against Cuba, which is comprised of a range of statutory measures, including the United States Liberty and Democratic Solidarity (LIBERTAD) Act of 1996 (the Helms-Burton Act). Canadian companies, including Canadian subsidiaries of US companies, are prohibited from complying with the Helms-Burton Act, creating the potential for significant intra-company conflict between Canadian subsidiaries and their US parents.

On 2 May 2019, the United States lifted the suspension of a private right of action under Title III of the Helms-Burton Act. This suspension now permits US nationals to bring civil claims for treble damages against foreign businesses and individuals for trafficking in property confiscated by the Cuban government after the 1959 revolution. Under FEMA, judgments of US courts until Title III are not enforceable in Canada and Canadian defendants may counter-sue in Canadian courts to recover any losses suffered from a Title III judgment.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Under the Foreign Extraterritorial Measures (United States) Order, Canadian corporations are required to give notice to the Attorney General of:

> *any directive, instruction, intimation of policy or other communication relating to an extra-territorial measure of the United States in respect of any trade or commerce between Canada and Cuba that the Canadian corporation, director or officer has received from a person who is in a position to direct or influence the policies of the Canadian corporation in Canada.*

Canadian corporations who commit an offence under FEMA are subject to fines not exceeding C$1.5 million or imprisonment for a term not exceeding five years.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct come to the attention of enforcement authorities and corporate management through a wide range of sources. Whistleblowers, internal or compliance audits and media reports are frequent sources of both internal and government investigations. In 2015, the Ontario Securities Commission (OSC) adopted a whistleblower policy to award up to C$5 million to persons who report securities law violations. In the first two years after the whistleblower policy came into effect, the OSC received approximately 200 tip-offs and it made its first three awards under the policy in February 2019 (totalling C$7.5 million).

Information gathering

21 Does your country have a data protection regime?

Canada has privacy laws at both the federal and provincial levels. The Personal Information Protection and Electronic Documents Act applies to federal government organisations and to businesses in provinces that do not have 'substantially similar' privacy protections. Canada does not have a broad data protection law equivalent to the European Union's General Data Protection Regulation.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

Contraventions of privacy laws are generally enforced through complaints to and investigations by commissioners appointed federally or provincially.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

Canadian privacy and data protection laws have not been impediments to internal investigations to date.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

There is no bright-line rule about whether an employer may monitor the communications of its employees on company-owned devices. An employee's contract of employment and company policies will typically provide that an employee's company computers, tablets and mobile phones are the property of the company and therefore may be monitored by the company without notice to the employee. If an employee has provided prior consent by signing such documents, courts will generally find that the employee's reasonable expectation of privacy is diminished.

Organisations that are covered by PIPEDA, or provincial privacy laws in Alberta, British Columbia or Quebec, are subject to additional restrictions regarding the collection and use of personal information, which can include information about topics such as an employee's health or financial situation. Although the various privacy laws differ in some respects, under

the strictest of laws, an employee's prior consent in the form of a contract of employment or signed company policies will generally permit the employer to monitor employee communications that contain personal information.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants are a feature of law enforcement in Canada.

Generally, a warrant to search a particular location may only be issued where there are reasonable grounds to believe that the search will yield evidence of the commission of an offence. The search warrant will outline the parameters of the search, including the date, time and the specific location (or locations) to be searched. An application for a search warrant must be supported by affidavit evidence establishing the requisite grounds.

If the requisite grounds for the search are lacking, or the parameters of the search authorised by the warrant are exceeded, the search will be unreasonable, in violation of Section 8 of the Canadian Charter of Rights and Freedoms (the Charter), which protects both individuals and corporations from unreasonable searches and seizures. At the investigative stage, an application to quash a search warrant can be brought after the search has been executed (there is usually not an opportunity to bring the application beforehand because the target of the search will typically only become aware of the search at the time the warrant is executed). If the application is successful, the fruits of the search may be returned to the party from which they were seized. If a prosecution is initiated, it is also possible to have evidence obtained from an unlawful search excluded pursuant to a pretrial application brought under Section 24(2) of the Charter.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

When a search warrant is being executed, the target being searched (or its legal counsel) may make a claim of privilege over privileged documents. In such circumstances, the documents will be sealed in an envelope and provided to the clerk of the local superior court. The investigating authorities and defence counsel may then negotiate a review process for the privileged records.

If the search warrant authorises the seizure or imaging of a computer, the target being searched (or their legal counsel) can still make a claim for privilege. A variety of methods may be used to review the computer data to protect the privilege. For instance, an officer not involved in the investigation may review the seized or imaged data to segregate the privileged records.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Section 11(c) of the Charter provides for a right against self-incrimination. It stipulates that any person charged with an offence has the right not to be compelled to be a witness in proceedings against that person.

Section 13 of the Charter also provides for a right against self-incrimination. It protects a testifying witness from compelled incriminating evidence that he or she provided being used against him or her in any other proceeding (except in a prosecution for perjury or for giving contradictory evidence). This protection is different from that afforded by the Fifth Amendment in the United States, under which a witness can refuse to testify.

A subpoena must be obtained to compel the attendance of a witness. For a judge to issue a subpoena, the party seeking the subpoena must be able to establish that the witness would probably, or is likely to, have material evidence to give.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Under the Criminal Code, it is an offence for an employer to discipline, demote or dismiss an employee in retaliation for that employee providing information to the authorities about a violation of federal or provincial law, or to threaten to do so. It is also an offence to do any of these things in an attempt to dissuade the employee from providing information to the authorities.

In addition, in recent years the provincial securities regulators in three provinces (Ontario, Quebec and Alberta) have introduced whistleblower programmes. Each of these provides various protections to whistleblowers who engage in protected activity, including assurances of confidentiality and anti-reprisal measures. For example, under the Ontario programme, employment agreement provisions that preclude an employee from engaging in whistleblowing activity are automatically void.

The Alberta and Ontario whistleblower programmes also provide a civil right of action for whistleblowers who have experienced reprisals. For example, under the Ontario programme, employees who engage in protected whistleblowing activity have a private right of action against companies that take reprisals. In any suit brought under the private right of action, the typical burden of proof is reversed such that the company must demonstrate that it did not take a reprisal against the employee. Remedies in such an action include the employee's reinstatement and payment to the employee of two times the amount of remuneration that the employee would have been paid but for the reprisal.

Of the three provincial whistleblower programmes, only the Ontario one offers monetary awards for information regarding misconduct. Under the Ontario programme, a whistleblower can receive up to C$5 million for submitting information about potential securities misconduct that leads to an enforcement action. In the first two years after the programme

launched, the Ontario securities regulator received approximately 200 tip-offs and, in February 2019, it made its first three awards under the programme (totalling C$7.5 million).

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

As a general matter, employees do not have any particular rights under employment law that govern how the company must interact with them during an internal investigation. However, if an employee is a whistleblower, the employee may have rights under local law against the company taking reprisals against him or her for the whistleblowing activity.

Apart from whistleblower protections, if an employee is treated unfairly and subsequently demoted or dismissed, that treatment may be a factor in wrongful termination proceedings instituted by the employee. Also, employees may be found to have a reasonable expectation of privacy in relation to their personal use of company computers, tablets and mobile phones. This expectation of privacy may preclude the company from voluntarily turning over the contents of these devices to law enforcement authorities for their use in a criminal investigation of the employee.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

An employees' rights under local employment law do not differ, and there are no particular steps that need to be taken by the employer, when an employee is implicated in, or suspected of, misconduct.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

It may be possible to dismiss an employee for refusing to participate in an investigation, particularly when the contract of employment imposes a duty on the employee to participate in an investigation.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

There is no mandatory process for conducting internal investigations in Canada. Independent investigations often begin with a document or work plan that sets out the subject matter and scope of the investigation. The work plan will generally evolve as the investigation progresses and its evolution is typically the subject of discussion between the investigators and the corporate authorities instructing the investigation.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Internal reports of potential illegal conduct should be passed on to management and, depending on the nature or severity of the conduct, to the board of directors. If a company lawyer becomes aware of certain types of misconduct, he or she may be obliged by local ethical rules to report that misconduct to management or the board, or both. The relevant corporate authority should consider whether immediate remedial action is required and consult counsel prior to deciding on the appropriate course of action, which can involve an internal investigation conducted by company personnel or an independent investigation by outside investigators. It is generally prudent to conduct a review and investigation of potential illegal conduct under the guidance and direction of counsel to preserve privilege on behalf of the corporation and to avoid inadvertent waivers of privilege before the scope and severity of the potential misconduct can be determined.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Note that such orders are only used against third parties and not the target of an investigation. If served with a preservation demand, a preservation order or production order, a company should immediately take steps to preserve and produce (as applicable) the data subject to the order.

If a company is unable to comply with the terms of the order in the time prescribed, the company may apply to the court to vary or revoke the order. Such an application may assist the company in obtaining more time to comply with an order (which can be broadly drafted) or address concerns about privileged documents. Notice of this application must be made to the officer named in the order within 30 days of the day on which the order is made.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

The obligation of a corporation to publicly disclose an internal or government investigation of illegal conduct varies according to a wide range of factors, including whether the corporation is private or publicly traded, the business activities of the corporation and the type of conduct in question. Public companies have disclosure obligations under Canadian securities laws with respect to 'material information'. Whether specific information regarding potential misconduct rises to the requisite level of materiality depends on several factors, both qualitative and quantitative. In certain sectors (e.g., financial services, consumer health and safety, and government procurement), companies are subject to legal or contractual obligations to disclose certain types of misconduct. In other instances, particularly those that have the potential to affect consumers, early public disclosure may be prudent for reputational reasons.

36 How are internal investigations viewed by local enforcement bodies in your country?

As a general rule, Canadian enforcement agencies welcome the efforts of corporations to address wrongdoing by officers, directors and employees, including conducting internal investigations. However, the posture towards internal investigations varies immensely from agency to agency and is affected by the safeguards that the company adopts to preserve the integrity of the internal investigation and the evidence collected.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Yes. Both attorney–client privilege and litigation privilege may attach to work-product produced in an internal investigation. Attorney–client privilege will protect communications made in furtherance of the provision of legal advice. Litigation privilege will attach to documents where the 'dominant purpose' of creating the document was anticipated or ongoing litigation. Neither attorney–client privilege nor litigation privilege will attach to documents that predate the investigation, or transcripts or factual summaries of interviews of employees or third parties not directly involved in instructing the lawyers conducting the investigation.

It is prudent to clearly define who the client is at the outset of the mandate (e.g., the corporation alone, the corporation and certain senior officers or a special committee of the board of directors) and who will be instructing the lawyers on behalf of the corporation. Documents should also be marked as 'solicitor–client privileged' or 'litigation privileged' and their dissemination should be restricted to the individuals directly involved in instructing the lawyers. Also, the client may choose not to have interviews recorded or verbatim transcripts prepared, but instead have their lawyers prepare impressionistic memoranda over which a tenable claim of litigation privilege may be made.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Attorney–client privilege applies to communications between an attorney and a client that are (1) expected to be confidential and (2) in furtherance of obtaining legal advice. The attorney–client privilege is held by the client and can only be waived by the client. This is the case irrespective of whether the client is a corporation or an individual. Privileged communications are shielded from disclosure indefinitely.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The fact that the lawyer giving legal advice is in-house (as opposed to external) counsel is irrelevant. A communication will be privileged if it is in furtherance of obtaining legal advice. Privilege will not attach to communications when in-house counsel is providing business

advice. Also, over-circulation of a document by in-house counsel can result in a finding that the communication is not privileged because it was not intended to be kept confidential.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Although the law on this issue is not settled in Canada, courts will generally apply the law of the forum to issues of attorney–client privilege. On that basis, when advice is sought from a foreign lawyer in relation to foreign law, attorney–client privilege will attach if the requirements of local law for the privilege are satisfied. Specifically, the communication between the foreign lawyer and the client must be made with the expectation of confidentiality and in furtherance of obtaining legal advice.

To support the strongest possible assertion of attorney–client privilege, it is best practice for domestic counsel (rather than the client) to undertake any communication with foreign lawyers during an investigation. In this way, the communications with the foreign lawyers are protected by privilege just as any other third-party and expert assistance engaged by counsel for the purposes of conducting the investigation.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

With the exception of provincial securities regulators, Canadian enforcement authorities do not generally request waiver of privileged information, and waiver of privilege is not generally required to obtain credit for co-operation. However, some agencies (particularly the RCMP) can be sceptical of extensive privilege claims even when they are well-founded. It is prudent in RCMP investigations of such matters as foreign corrupt practices, procurement fraud, sanctions and export control violations, to consider whether appropriate waivers of specific privileged information may be beneficial to the corporation.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The concept of limited waiver of privilege exists in Canada, but the circumstances in which a corporation can successfully assert that it intended a limited waiver are uncertain. Although the precise contours of the limited waiver doctrine are unclear, when the production of privileged information is required by statute, and the privileged information is produced for that purpose, the doctrine of limited waiver will apply.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

If the preconditions for the assertion of privilege exist, and it is clear that only a limited waiver for a specified purpose was intended, privilege could possibly be maintained in Canada.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege does exist in Canada. Common interest privilege may be invoked if a party voluntarily discloses a privileged document to another party who has a common interest in the subject matter of the communication or in the litigation in connection with which the document was created. For common interest to exist, the parties must share a common goal, seek a common outcome or have an identical and shared interest. The common interest does not need to exist at the time the privileged document is created, so long as the common interest exists at the time the document is disclosed.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Yes, as a general rule, third-party and expert assistance engaged by counsel for the purposes of conducting an investigation, such as forensic accountants and investigators, data recovery services, translation services and document review, is covered by privilege.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes. Witness interviews are generally a key part of internal investigations.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Internal witness interviews may be covered by litigation privilege, provided that the interviews are for the dominant purpose of existing or contemplated litigation. Because litigation privilege does not protect underlying facts from disclosure, a successful assertion of privilege can only be made regarding impressionistic summaries prepared by the lawyer. Attorney–client privilege will also attach to interviews of key individuals involved in instructing the lawyers.

Reports prepared by lawyers as part of an internal investigation may also be attorney–client privileged, provided that (1) the report is delivered in the context of a attorney–client relationship, (2) the report is prepared for the purpose of providing legal advice, and (3) the report is prepared and delivered with the expectation of confidentiality.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

It is generally considered prudent to give an employee an *Upjohn*-type warning, although the issue of whether such a warning is required has not been considered by a Canadian court. In addition, if an employee is to be interviewed by a lawyer on behalf of the employer, local ethical rules require the lawyer to make it clear that he or she is acting on behalf of the employer and not for the employee, and if the employee subsequently seeks legal representation, the lawyer cannot interview the employee except with the express consent of the employee's lawyer.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Documents may be put to the witness. The interview may be recorded, but the recording will not be privileged. Employees should be advised that the interviewing lawyer acts for the employer and so the employee may seek their own legal representation. If the employee retains a lawyer, they cannot be interviewed except with the express consent of the employee's lawyer. Such an interview would generally take place in the presence of the employee's lawyer.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

There is no general obligation to report misconduct to law enforcement authorities. However, companies in certain sectors (e.g., financial services, consumer health and safety, and government procurement) are subject to legal or contractual obligations to disclose certain types of misconduct to the appropriate authorities.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

A company might be advised to self-report if it is likely to receive credit for doing so and the underlying misconduct is likely to come to the attention of law enforcement. Formal credit for co-operation programmes have been established by the OSC for securities regulatory offences and by the Canadian Competition Bureau for offences under the Competition Act. Other agencies may have also been known to give credit or decline to prosecute in the case of self-disclosure, for example in matters involving economic sanctions, export controls and foreign corruption. With recent legislation that provides for deferred prosecution agreements, it is possible that the circumstances under which voluntary self-reporting would be advisable will expand. The Public Prosecution Service of Canada has not entered into any such agreements to date.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

Both the OSC and the Canadian Competition Bureau provide guidance in respect of how to self-report under their credit for co-operation programmes.

Under the OSC programme, an organisation will, typically through counsel, contact the staff of the OSC to self-report and offer its co-operation. The staff will generally require the organisation to disclose particulars of the conduct at issue, including by forwarding documentation, providing fact witnesses for interviews and responding to the staff's questions. An organisation's co-operation under the programme can result in the staff agreeing to take no enforcement action against the organisation, a settlement agreement in which the organisation makes no admissions of liability or a reduction in sanctions.

The Canadian Competition Bureau self-reporting regime comprises two programmes: the Immunity Programme and the Leniency Programme. Under the Immunity Programme, organisations that are the first party to self-report a competition offence may be eligible under the programme for complete immunity from prosecution. To benefit from the Immunity Programme, an organisation must provide complete, timely and ongoing co-operation to the Bureau at its own expense. Under the Leniency Programme, organisations that are not the first party to self-report a competition offence may be eligible for leniency in sentencing as long as they have terminated their participation in the activity at issue, agreed to plead guilty to the offence at issue, and agreed to co-operate fully and in a timely manner with the Bureau.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

The company is likely to approach the authority conducting the investigation to understand the allegations. Discussions may be entered into to assess whether there is information the company can provide that will enable it to avoid a prosecution, either because the information refutes the allegations or establishes that a prosecution is not in the public interest (i.e., because the company has undertaken an internal investigation and subsequent remedial action).

54 Are ongoing authority investigations subject to challenge before the courts?

In theory, investigations can be challenged through an application for judicial review of administrative action. Such an application is likely to be successful only if the law enforcement agency undertaking the investigation clearly lacks the lawful authority for doing so.

In a recent high-profile example, engineering company SNC-Lavalin Group challenged by way of judicial review the decision of prosecutors not to offer it a deferred prosecution agreement (also known as a remediation agreement) for charges of bribery of foreign government officials. SNC-Lavalin sought to have the court compel prosecutors to negotiate a remediation agreement with the organisation in good faith. In a March 2019 decision, the court refused the application, concluding that the decision not to offer a remediation agreement falls within the ambit of prosecutorial discretion and so is not reviewable.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

As a first step, local counsel should be retained in both jurisdictions and counsel in each jurisdiction should serve as the contact point for the local authorities. Counsel may then wish to make enquiries directed at determining whether the action is coordinated, taking care not to reveal that they are the subject of the investigation in the other jurisdiction if prohibited from doing so under local law. If it is confirmed that the action is coordinated, it would be prudent to consider whether a consistent disclosure package can be negotiated. If prohibited from revealing the existence of the investigation, it is likely that this can only be done through

the agency in the locality that prohibits revealing the existence of the investigation. Generally, in Canada, there is some scope for negotiation around what is to be produced, even if there is a court order compelling production.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Yes. A production order would apply to information in the company's control anywhere in the world.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Canadian law enforcement agencies can share information with foreign agencies pursuant to various arrangements, both formal and informal. For example, information can be provided to a foreign agency through a formal mutual legal assistance request managed by the International Assistance Group of the federal Department of Justice. Certain agencies also have formal arrangements with their foreign counterparts that provide for information-sharing and assistance (e.g., the Competition Bureau has co-operation agreements with the US Department of Justice and Federal Trade Commission, the European Commission and other foreign competition authorities). The provincial securities commissions have memoranda of understanding with the US Securities and Exchange Commission that authorise information-sharing in specific circumstances. Other agencies (including the RCMP) have close relationships with foreign enforcement agencies and can contact their counterparts for assistance and information that is not confidential or otherwise restricted by the relevant foreign government.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Yes. Disclosure will be restricted to parties facing a criminal or regulatory prosecution arising out of the investigation. Disclosure to third parties, such as in a class action, will generally only be made pursuant to a court order.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Canadian enforcement agencies are familiar with foreign data protection laws that restrict disclosure of information. While referencing those laws is important in the discussion of production expectations and timing, it is often useful to obtain a foreign legal opinion to determine whether the foreign law prohibits the disclosure of the precise information that is being requested by Canadian authorities.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Canada does not presently have a traditional blocking statute that prohibits disclosure to foreign authorities or persons except as permitted by treaty.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Confidentiality will attach to information that is compelled and information that is produced voluntarily. When information is produced voluntarily, a company is generally precluded from challenging the admissibility of that information as evidence in a subsequent prosecution against it at the instance of the regulator. Disclosure to third parties, such as in a class action, will generally only be made pursuant to a court order.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Companies face fines, probation, disgorgement and debarment. Directors, officers and employees face fines, probation, disgorgement and imprisonment.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

The federal government maintains an integrity regime that provides for suspension and debarment of suppliers of goods and services to the government of Canada if they have been charged with or convicted of designated offences in Canada or in a foreign jurisdiction. Designated offences include fraud, corruption, price-fixing and bid rigging and other economic crimes. The integrity regime provides for mandatory debarment for 10 years if a company has been convicted of a designated offence. The debarment can be reduced by up to five years if the company enters into an administrative agreement with Public Services and Procurement Canada (PSPC). Suspension and debarment are discretionary if an affiliate of the company is charged or convicted in a foreign jurisdiction, and depend on a determination by the PSPC as to whether the Canadian company had any role, or participated, in the foreign offence. Companies can, in certain circumstances, avoid suspension pending trial by entering into an administrative agreement with the PSPC to implement or maintain agreed compliance measures.

Quebec and New Brunswick are the only provinces to maintain a similar suspension and debarment regime. The Quebec regime is administered by the provincial securities regulator and applies to both private and publicly traded companies. The New Brunswick regime applies to prospective provincial government suppliers and predicated on convictions of enumerated offences, including economic crimes and foreign corrupt practices.

64 What do the authorities in your country take into account when fixing penalties?

The fundamental principle of sentencing is that the sentence or penalty should be proportionate to the gravity of the offence and the degree of responsibility of the offender. There is a whole host of other aggravating and mitigating factors prescribed by statute and that have been recognised at common law. Among the most commonly considered are whether the company or individual entered into an early resolution, whether they co-operated with the authorities in the investigation, and whether they voluntarily repaid ill-gotten gains or otherwise voluntarily undertook remedial action.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Canada has introduced deferred prosecution agreements (referred to as remediation agreements) as a result of amendments to the Criminal Code that came into force on 19 September 2018. A remediation agreement is defined as 'an agreement between an organisation accused of having committed an offence and a prosecutor, to stay any proceedings related to that offence if the organisation complies with the terms of the agreement'. Remediation agreements are subject to judicial approval and are available for specified offences, including foreign and domestic corruption, fraud, stock manipulation and insider trading. The Public Prosecution Service of Canada has not entered into a remediation agreement to date.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Under recent legislation in Canada that introduced remediation agreements, once a court approves a remediation agreement, that agreement must be published by the court unless it is satisfied that non-publication is necessary for the proper administration of justice. In determining whether to publish a remediation agreement, the legislation provides that the court must consider, among other things, the prevention of any adverse effect to any ongoing investigation or prosecution.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Settlements attract deference from courts and regulatory authorities, but they are generally not bound by them. Also, when making admissions as part of a settlement, the admissions should be qualified as being for that purpose and not for any other purpose. Once a settlement is entered into, it is likely that litigation privilege will no longer apply to documents prepared for the purpose of the regulatory proceeding.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

The use of external corporate compliance monitors has historically been limited to non-criminal regulatory matters. Provincial securities regulators and self-regulatory organisations will sometimes require that a company engage an independent monitor to assist with remediating compliance deficiencies identified as part of a regular compliance review or misconduct investigation. These regulators usually require that they approve the organisation's selection of monitor and set the monitor's mandate. The monitor will be given reasonable access to the organisation's books and records as is necessary to fulfil its mandate and will typically be required to report its observations and recommendations to the regulator.

The 2018 legislation in Canada that introduced remediation agreements may result in an expanded use of monitors in the resolution of criminal matters. Under the new legislation, a prosecutor may require the appointment of an independent monitor for the organisation as a condition of a remediation agreement. The independent monitor is charged with verifying and reporting to the prosecutor on the organisation's compliance with remedial measures during the term of the remediation agreement. Prosecutors must approve the organisation's selection of monitor and the organisation is obliged to co-operate with the monitor and pay its costs. Since the Public Prosecution Service of Canada has not yet entered into a remediation agreement under the new regime, no monitors have been imposed to date.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Yes. In some instances, such as for certain violations of securities regulations or the Competition Act, the applicable statutes provide for a private right of action. Access to the authorities' files is possible through a court order.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Publicity at the pre-charge stage is generally very limited. Law enforcement agencies will generally not release information voluntarily unless there is a particular investigative objective to be achieved by releasing the information. However, it is possible that the media will be able to gain access to information through court records of applications for search warrants. Although these records are often sealed, an application to unseal them can be brought in high-profile cases (which is often done).

Once a charge has been laid, court proceedings are open to the public and, with few exceptions, the proceedings can be reported by the media.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Yes. However, corporate communications should be vetted by the company's lawyers as they are admissible against the company in court proceedings.

72 How is publicity managed when there are ongoing related proceedings?

A corporate communications firm may be engaged, but if the company is a party to the proceedings, or could be a party to future proceedings, its communications should be vetted by the company's lawyer to ensure that they do not compromise the company's position in those proceedings.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

A public company will be required to disclose an investigation or a settlement where it constitutes a 'material fact' or a 'material change' under applicable securities laws.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Canada's federal government held parallel public consultations in 2017 and 2018 on expanding measures to address corporate misconduct and updating its policies on debarment from public procurement. The consultations resulted in the introduction of remediation agreements (deferred prosecution agreements) in the Criminal Code in September 2018. The consultations also led to the publication in November 2018 of draft amendments to the federal Integrity Regime, which governs eligibility, suspension and disqualification for federal procurement. The amendments propose, among other things, to eliminate mandatory debarment upon conviction of a predicate offence and to leave the period of debarment to the discretion of the Integrity Regime Registrar. The government has indicated that it intends to adopt the amended policy at a future date.

Canada has been broadly criticised by the Financial Action Task Force, and other international and domestic organisations, for its lax anti-money laundering legislation and enforcement. The federal and provincial governments issued a joint statement in June 2019 committing to improving beneficial ownership transparency to combat money laundering and financial crime. The statement contemplates consultations on a public beneficial ownership registry. A timeline for the consultations has not yet been announced.

10

Chile

Andrés Jana and Karen Werner[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The highest-profile corporate investigation currently under way in Chile is *Corpesca*, a criminal case against a Chilean fishing company (Corpesca), loss of privilege senator Jaime Orpis and former congresswoman Marta Isasi.

The investigation relates to a scandal that affected the entire political spectrum in 2015 with regard to the illegal financing of electoral campaigns by large businesses. It involves charges such as illegal financing of electoral campaigns, bribery and tax fraud, among others. It also involved important Chilean companies, such as Penta and SQM (one of the country's largest privately owned mining companies), and several politicians from all sides of the political spectrum.

However, Chilean prosecutors have only pressed charges in criminal court against Corpesca, Senator Orpis and former congresswoman Isasi. Therefore, and notwithstanding that the political scandal affected several politicians and businesses, currently Corpesca is the only Chilean company that could face criminal sanctions arising from the 2015 scandal, and Senator Orpis could be the first Chilean politician to face criminal sanctions, risking a jail term.

2 Outline the legal framework for corporate liability in your country.

Law 20,393 (enacted in 2009) provides that corporations are criminally liable for certain criminal offences carried out by their owners, managers and employees acting in the interests of the corporation when this is a consequence of breaching duties of supervision (Article 3,

1 Andrés Jana and Karen Werner are partners at Bofill Mir & Alvarez Jana.

Law 20,393). In practice, this means that a company might be liable if it failed to develop and implement an effective compliance programme with the aim of preventing such offences from being carried out.

The legal framework operates under some express offences established in Law 20,393. In its original form, the law limited the offences to those under which Chile had international duties of criminal enforcement (i.e., terrorism funding, foreign bribery). However, the scope has expanded to certain general offences such as bribery, several environmental crimes and, lately, some forms of corporate fraud.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The primary enforcement authorities relating to corporations are: the Tax Authority (SII), the Financial Market Commission (equivalent to the US Securities and Exchange Commission) and the Antitrust Prosecution Office. The Criminal Prosecution Office (Ministerio Público (MP)) centralises all criminal enforcement competences. Each office has jurisdiction over its own subject matter.

In general, there are no normative rules or protocols to coordinate and distribute activities between the different offices. The MP has some limitations in its jurisdiction, but these are rare.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Chilean law does not generally provide for limitations of this kind. Discretionary decision-making by prosecutors and officials in the different agencies, acting under the traditional sources of motivation and constraint found in institutions of this kind, determines these outcomes. In some cases, the agencies have internal guidelines regarding the decision-making process. In the case of the MP, two General Instructions provide some guidance about the content of the law, but it does not go beyond the formal text of the statute in establishing certain criteria to prosecute a corporation.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

The legal regulation of criminal enforcement does not provide for subpoenas requesting documentary information from private parties. In practice, a private party that receives a subpoena requesting documents from the authority can refuse to comply. Prosecutors are then likely to ask a judge to grant them seizure powers of those documents, according to Article 217 of the Criminal Procedure Code.

Subpoenas to give testimony in the context of a criminal investigation are mandatory. All witnesses must comply with at least answering the summons. They can only refuse to testify on a given question under privileges against self-incrimination or professional secrecy.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Leniency agreements have started to appear in different areas of Chilean law. While there is no general criminal law provision regulating immunity and leniency, a prosecutor may offer to ask for diversion or other benefits in the context of a plea bargain or in the case of minor felonies.

The particular areas that provide for leniency agreements include antitrust regulation, financial market regulation, criminal law dealing with corruption, and some forms of organised crime.

In the case of corporate criminal liability, a defendant can also receive some benefits if he or she makes significant contributions to the process.

7 What are the top priorities for your country's law enforcement authorities?

The scale of national attention on the *Penta Group* and *SQM* cases are indicative of the interest in incidents relating to tax evasion. Nevertheless, in the past few years, the SII has become reluctant to allow the MP to prosecute tax evasion offences in high-profile cases. Law enforcement officials seem to prefer to prioritise corruption and corporate frauds. This focus was given a boost with the enactment of Law 21,121 in November 2018, which considerably expanded the scope of these types of offences.

Law enforcement agencies are also focusing on antitrust behaviour. During the past decade, the work of antitrust enforcement agencies and the Antitrust Tribunal in Chile has become increasingly relevant.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Entities that receive personal data must ensure that the rights of the data subject are safeguarded and transmission of information is related to the tasks and purposes of the participating organisations. Also, if there is a request for personal data via an electronic network, the following information must be recorded: (1) the enquirer's identity, (2) the motivation and purpose of the request, and (3) specifics of the personal data being transferred.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Although cybercrime regulation in Chile is old and incomplete, some law enforcement authorities do have departments that specialise in cybercrime matters, such as the Chilean Investigations Police. The National Prosecution's Specialised Office on Economic Crimes includes cybercrime as part of its remit. However, few specific cybercrime offences are included in criminal legislation. Cybercrime is instead prosecuted under general offences (such as fraud) that are committed through the internet (e.g., phishing).

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Criminal laws operate under the principle of territoriality established in Chile's Constitution. Extraterritorial liability is only allowed by law in some specific cases. There are some regulations of extraterritorial effects relating to offences between Chilean parties, conspiracies that affect the Chilean market, several types of sexual offences, offences perpetrated by Chilean officials overseas against the state, and foreign bribery.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Whereas coordination with foreign offices was virtually non-existent 15 years ago, some law enforcement agencies have units that are responsible for international co-operation. Lack of regulation and similarity with the regulations of other countries create difficulties in cross-national cases. For example, Chilean law has a fragile framework for asset freezing and forfeiting, which has created problems in attempts to recover assets overseas and to comply with asset recovery demands.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Chilean criminal law recognises double jeopardy as a general principle. Article 13 of the Criminal Procedural Code (CPP) recognises the effects of criminal judgments made by a foreign court. Thus, criminal law impedes double jeopardy. The only exception provided for is in cases that the Chilean judge deem to be mock trials.

In the past few years, anti-piling on has been on a hot topic of debate. Since its judgment STC 244 of 1996, the Chilean Constitutional Court explicitly acknowledges that the general principles of criminal law also apply to the sanctioning powers of other agencies, including the protection against double jeopardy. The exact conditions under which such provisions apply is obscure, however. In its judgment STC 496 of 2006, the Chilean Constitutional Court declared that the principles of criminal law apply only with 'nuances', without specifying them. In the past few years, both the Constitutional Court and the Supreme Court have discussed several cases of double jeopardy, in particular regarding securities offences: both criminal law and administrative law provide for sanctioning powers for such offences. The general conditions under which the anti-piling on rule works are unclear.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not common in Chile.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Authorities are likely consider them and weight them depending on the ruling by the foreign authority. However, there is no legal regulation on this issue.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Criminal law provides for the traditional types of sanctions that can be found in any penal regime, imprisonment and fines being the most common. Under Chilean law, people can go to prison if the nominal penalty goes beyond three years' imprisonment (in some cases, five years) and the defendant has not been convicted of a crime in the past 10 years or of a simple felony in the past five years.

In cases of white-collar crime, defendants are unlikely to serve time in prison as they will not generally have prior convictions, and penalties rarely go beyond three or five years in these cases. This situation may change with the enforcement of Law 21,121, as the nominal penalty for bribery offences has been increased. Although Law 21,121 is already applicable in Chile, there are been no convictions since November 2018, when it was published.

Criminal fines have been traditionally low. However, this has changed regarding a corporate's liability because fines can now be as much as 300,000 *unidades de fomento*.

Individuals may also face several prohibitions to exercise public duties and to serve as directors or managers in open corporations. Corporations may also be punished by being prohibited from negotiating contracts with the state and losing benefits obtained from such contracts. The most severe punishment for corporations is dissolution.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Criminal and administrative enforcement has increased in the past decade as a result of different scandals and a general change in public opinion. The general approach in criminal enforcement has also become more professional, taking into account the number of specialist departments that now exist. However, in certain areas (asset forfeiture, for example), it still remains ineffective.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Several institutions, including the MP, have international co-operation departments.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Not that we are aware of.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

This does not apply.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Although local authorities claim that their screening and reporting mechanisms are robust, most major corporate scandals have been initiated by media reports, self-reporting in the context of an investigation and whistleblowing.

Perhaps the best illustration of this is the *Penta* case, which started with an investigation into possible tax evasion, in which an internal official had collaborated. It gained ground when one of the individuals involved confessed to being part of the scheme, alongside a senior manager within the Penta Group. Feeling betrayed by his employers after being fired, that individual co-operated with the authorities and provided critical information.

Information gathering

21 Does your country have a data protection regime?

Law 19,628 provides a general regulation on the matter. As the regulation stems from before the data revolution of the last few decades, it is generally considered obsolete.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

Chile does not have an agency that is responsible for the surveillance of compliance of the enforcement of personal data protection regimes. Instead, general courts of justice oversee the protection of data under the Data Privacy Law in the following circumstances: (1) a particular procedure before civil courts is considered in the Data Privacy Law for breaches to said Law, and (2) a constitutional protection action can be filed if a breach affects the constitutional right to the protection of personal data, which must be used in accordance with the law.

Bill No. 11,144-07, which amends the Data Privacy Law and is currently being reviewed in the Senate, states, among other things, the creation of a Personal Data Protection Agency, which must certify that the breach prevention model and the compliance programme that the Bill also sets forth, meet the requirements provided in the new law and its regulations, and shall monitor compliance therewith.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

Lack of regulation is the most pressing issue. The status of basic information, including employees' email, is unclear and has been the subject of discussions about their legal and constitutional status when used both to prevent and to prosecute criminal offences.

Discussions are generally based simply on the general rules of criminal law (necessity or less heinous defences) or of constitutional law (intimacy rights).

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

See question 23. Employers tend to give consent for the use of communications for such purposes in employment contracts, but the validity of such clauses is arguable.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants need to be authorised by a judge and, generally, are effected after giving notice. With due cause, prosecutors can request that prior notice need not be given.

Authorities executing search warrants have to maintain strict custody of, and record, all seized items. They are prohibited from seizing communications that fall under the umbrella of professional secrecy.

A company can request that excessive behaviour should cease by presenting a constitutional action to consider a violation of fundamental rights. Moreover, a company can formally request consideration that the evidence obtained is null and void.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Authorities executing search warrants must safeguard and record all seized items.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

All witnesses are obliged to answer a summons and testify. However, if there is a risk of self-incrimination, or if a person's testimony could affect spousal or family relationships, or professional secrecy (such as attorney–client privilege), witnesses can refuse to testify, although they still have to answer the summons.

Witnesses who do not answer a summons can face fines and arrest. All witnesses, except defendants and their close relatives, can face charges of false testimony.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Chile does not have a specific whistleblower regulation in respect of employment matters. However, there are regulations relating to sexual harassment at work (Article 211-A et seq., Labour Code).

Internal claims (apart from sexual harassment) are not lawfully regulated in respect of whistleblowers but a company could create its own incentives. However, if an employee makes specific allegations before the Labour Department or labour courts, the employer cannot dismiss them (Article 485, Labour Code).

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employment law does not confer exclusive rights to employees who participate in an internal investigation. If it is an investigation conducted by the Labour Department, individuals may have protection against dismissal. Employment law does not distinguish between employees, officers and directors.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Each case must be considered on its merits. If the matter relates to sexual harassment, or another form of harassment in the workplace, in the first instance, the suspect should be separated from the injured party. That may represent a suspension of the suspect's duties or relocation from the usual place of work. In any case, the employer could not stop paying the salary while the investigation is taking place.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

There is no scope for compelling someone to participate in an internal investigation. The only possible cause for dismissal is when a suspect is declared guilty of sexual harassment, or another form of harassment in the workplace (Article 260(1)(b) and (f), Labour Code).

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Internal investigations are a relatively new phenomenon, so there are few common practices in place. However, before starting any investigation, companies usually prepare documents

containing the claimant's name, the accused's name and a summary of the accusation. It also may contain details regarding the investigation process, such as the dates involved and details of the investigation process.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Reporting can make leniency rules applicable. In labour cases, such as matters relating to sexual harassment, the affected employee can request the intervention of the Labour Department. In these circumstance, the company should provide the information requested by the authority.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

There is no specific labour regulation. However, subpoenas from the labour authority must be met. Also, the employer has a legal duty to store all labour documentation.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

In labour issues, the only applicable situation is with sexual harassment cases. If a company carries out an internal investigation, the results of it should be sent to the Labour Department within 30 days of the date of the initial claim.

36 How are internal investigations viewed by local enforcement bodies in your country?

Regarding labour issues, such as mobbing or sexual harassment, usually, they are resolved through internal investigations, which is permitted by the Labour Code.

Regarding sexual harassment procedures, the law includes minimum requirements such as deadlines and investigations carried out according to due process.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

There is no specific rule regarding internal investigations within a company. However, the attorney–client privilege is a general rule established in the Lawyer Ethics Code. A lawyer must always maintain and protect a client's confidentiality.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

There is no difference between an individual client or a company. The holder of the privilege is the lawyer. The main principles of the attorney–client privilege are as follows:

- strict confidentiality (the scope for which extends to all the information that an attorney receives from a client);
- the attorney's right to recognition of privilege;
- prohibition on disclosure;
- duty of care towards all information received or disclosed;
- duty of care towards people who assist an attorney; and
- indefinite duration.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The law does not distinguish between, and applies equally to, in-house and external counsel. The attorney–client privilege generally applies, and is extendable to law firms.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Lawyers in Chile should comply with the rules established in the Lawyers Ethics Code.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

The Lawyer Ethics Code only establishes the duty to waive the attorney–client privilege to avoid or impede a crime. Also, it provides for the possibility to waive in specific instances, such as to avoid serious risks of death or serious injury, to obtain advice from another lawyer with the duty of confidentiality, or to comply with a duty of law. Co-operation is not established as a specific waiver.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Chile does not regulate this issue expressly. The Lawyers Ethics Code only provides for those instances when a lawyer must or can waive the right.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Attorney–client privilege should be maintained in Chile.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

No, the privileges only apply regarding the client.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Yes, the Lawyers Ethics Code establishes a broad scope of privilege, and relates to all information that has been received by a client or third parties that relates to issue raised by the client.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

This is not addressed by Chilean law, so it is common practice for witnesses to be interviewed. In fact, it is one of the most widely used forms of evidence in an internal investigation.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

This is not addressed by Chilean law. Privileges are claimed in practice, but their effects are unclear.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There is no specific regulation on this issue. However, the main requirements relate to the confidentiality of communications and data protection. Since there is a lack of common standards regarding interviews, the most prudent way for a witness to handle an interview is to identify straight away any risk of self-incrimination or conflict of interest.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

There is no specific regulation in respect of such interviews, but typically those present are the interviewer and the witness. Interviews are sometimes recorded. Relevant documents are presented to the witness depending on the case. It is not typical for an employee to have legal representation.

The lack of common standards means that, in general, there is no requirement for attendance by an attorney other than the company's attorney, but an employee may wish to do have their own representation. The company attorney should make it clear that he or she is not acting for the witness to avoid any confusion on the matter.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

The moral obligation to report misconduct is rare in Chilean law. As a matter of doctrinal law, however, there may be a case for criminal liability for omission if the misconduct continues after the party becomes aware of it.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

As regards antitrust, self-reporting to the relevant law enforcement authority is crucial in cases of collusion. Articles 39 *bis* and 63 of Decree Law 211 establish and regulate a leniency programme. According to Guidelines issued by the Fiscalía Nacional Económica (the national competition authority responsible for defending and promoting competition), the programme allows individuals or companies who have engaged in collusive conduct to be exempted from the relevant sanctions, or to have them reduced, provided that the applicant provides information that can be used to prove the conduct and identify the parties involved. Therefore, if a client has participated in a collusion scheme, self-reporting would be advisable.

In matters other than collusion, there are no rules regarding self-reporting. Usually, if it is an important issue, it will be disclosed as material information, or as a note in the financial statements. Further, companies usually name one specific internal authority for the resolution of a case. In most cases, a company's managing director will determine whether the matter in question is sufficiently important.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

Given that there are no incentives to self-report to law enforcement authorities, it is not usual for companies or compliance officers to make a self-report (except in cases of collusion). However, the formal method would be to submit a writ before the criminal court. If deemed admissible, the writ of self-report would be assigned to the MP for further investigation.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

There is always a chance to have a dialogue with the authorities and to request a meeting through public processes as regulated by law, either before or after charges are brought.

54 Are ongoing authority investigations subject to challenge before the courts?

Yes.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Two main principles in the Chilean legal system are the (1) territoriality and (2) relative effects of the awards. Thus, negotiating a consistent disclosure package might not be very useful, considering each of the different cases. Extraterritorial liability is allowed by law only in certain specific cases, such as offences between Chilean people, conspiracies that affect the Chilean market, a number of sexual offences, foreign bribery, among others.

Individuals may also face restrictions or bans, such as exercising public duties or serving as a director or manager in public corporations. Corporations may also be punished by being barred from negotiating contracts with the state and losing the benefits obtained from such contracts. The most severe punishment for corporations is dissolution.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

According to Chilean law, companies must disclose all the documents requested by the authorities that are in their possession or to which they have access. However, should a company decide not to present requested documents, the only sanction is that the company is not allowed to use those documents in its own favour.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

In private law, this is not usual. In criminal law, however, information regarding border control, international crimes, among other things, is routinely shared. For example, the International Co-operation Unit of the MP does provide information to international law enforcement agencies. The Financial Analysis Unit, a government agency, also provides information when required.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Prosecutors must keep all their internal proceedings and investigations secret from third parties while there is an ongoing investigation.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

We would present a statement in response, asserting that, according to the country where the documents are available or were produced, it is not possible to obtain them. In any case,

according to Chilean law and under Chilean jurisdiction, the only sanction on a party that does not produce documents is a ban on using those documents in its own favour.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Not that we are aware of.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Both criminal and civil proceedings are public in Chile. In criminal law, during the course of an investigation, all the evidence produced should be treated as confidential; however, once it has been produced in open court, it becomes public information, unless a particular exemption applies.

There is no difference between voluntary or compelled production of documents in private law. In criminal law, however, if a defendant co-operates with the authorities, it might gain some benefits, such as a reduction in penalties or lesser charges.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

The usual sanctions for misconduct are imprisonment and fines.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

There are unlikely to be any restrictions because of the principle of territoriality.

64 What do the authorities in your country take into account when fixing penalties?

Sentencing is underdeveloped in Chile. Judges will generally apply the minimum prison sentence that the law allows. Regarding fines, there is more room for discretion, though even here there is no clear guidance. In general terms, a penalty might be more severe to reflect the seriousness or scale of the infringement, or in the case of a repeated infringement.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

These are available only in cases of diversion agreements and plea bargains.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Even though prosecutors must keep all their internal proceedings and investigations secret from third parties, in general terms, all criminal proceedings are public unless a judge rules to the contrary.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Companies should confirm that the law enforcement authority is authorised to sign the agreement (proxies), that the settlement covers every aspect of the case, that the law enforcement authority is waiving any actions regarding the same issue, and that the agreement is legally usable and confidential.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Authorities seldom use external corporate compliance monitors as an enforcement tool.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Private parties can file private actions, but they will generally not be able to go beyond a certain point if the prosecutor decides to dismiss the case.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Prosecutors must keep all their internal proceedings and investigations secret from third parties (Article 182, CPP). All procedures that take place before the courts are public unless a judge rules to the contrary.

Despite the duty to keep all proceedings secret from third parties to avoid reputational damage, prosecutors are known to inform the press when it is beneficial to the case. Although measures have been taken to avoid this taking place, higher MP authorities have been unable to police such misconduct effectively.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It has become common, and sometimes essential, in corporate cases involving potential criminal liability for a company to use a public relations firm. However, internal communications are usually dealt with by a company's managing director or communications manager.

72 How is publicity managed when there are ongoing related proceedings?

There is no rule regarding this issue. If it is an important matter, it will be duly disclosed as material information, or as a note in the financial statements. It is usually the managing director who determines whether a matter is sufficiently important for details to be published.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

As regards listed companies, if a settlement is in relation to 'material information', in accordance to the relevant law, it must be disclosed immediately. Further, the law establishes certain cases where disclosure may be withheld temporarily.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Law No. 21,121 has provided for a significant change in local regulation. It is likely that in the next few years, there will not be any further similar changes, except in some specific areas, such as cybercrime and data protection, which are key objectives for local authorities as regards regulations.

11

China

Kyle Wombolt, Christine Cuthbert, Mark Chu and Tracey Cui[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

China's gift-giving culture (*guanxi*), combined with an abundance of state-owned enterprises (SOEs), pose clear corruption risks. China has a unique enforcement environment and corporate investigations take many forms. The local domestic market is dominated by SOEs and President Xi Jinping's anti-corruption campaign has targeted them, with large-scale investigations in a number of industries. However, these investigations have generally resulted in prosecutions and disciplinary actions against senior management personnel, rather than the SOEs themselves. For example, in 2018, both the former president of the People's Insurance Company of China and the former general manager of the state-owned conglomerate, Sinochem Group, were separately prosecuted for corruption.

In relation to multinational corporations (MNCs), the highest-profile corporate investigation to date remains that of British pharmaceutical giant GlaxoSmithKline (GSK) in 2014. The trial resulted in GSK itself, and senior executives of its China branch, being found guilty of bribery. GSK was penalised with a fine of US$492 million by a Chinese court.

The pharmaceutical sector remains under considerable scrutiny by regulators and authorities, with a number of investigations under way. Of particular note is the announcement by China's Ministry of Finance in June 2019 that 77 major pharmaceutical companies would undergo an audit over a two-month period, including the local branches of MNCs Sanofi, Eli Lilly & Co and Bristol-Myers Squibb Co. This announcement followed a filing by Kangmei

1 Kyle Wombolt is a partner, Christine Cuthbert is a senior associate, and Mark Chu and Tracey Cui are associates at Herbert Smith Freehills.

Pharmaceutical Co that its 2017 results contained multiple 'accounting errors', which raised potential issues of corruption and bribery.

There have also been a number of significant corruption investigations announced in the technology sector in recent months, including suspected corruption by individual employees of Meituan Dianping and the head of the video platform Youku.

Activity in China has also been the focus of more US corporate enforcement actions than conduct in any other country since the enactment of the Foreign Corrupt Practices Act in 1977. These US-driven investigations have led to an increased number of concurrent or follow-on investigations by China's criminal law enforcement authorities and regulators.

2 Outline the legal framework for corporate liability in your country.

Corporate entities can be held criminally liable for giving bribes to state personnel (and persons closely associated with state personnel), non-state personnel, foreign officials, and state entities and enterprises. Corporate criminal liability generally attaches where the relevant misconduct is an exercise of 'corporate will' (i.e., the decision to engage in misconduct was a group decision or was made by the personnel in charge). For example, in the high-profile GSK prosecution, GSK was found guilty on the basis that its management encouraged bribery of doctors, hospitals and other institutions for the benefit of the corporate entity.

Amendments to the Anti-Unfair Competition Law (AUCL), which came into force in January 2018, revised the legal framework for civil bribery. Business operators, which includes corporates, can be found liable for civil bribery offences if they bribe individuals or entities to seek transaction opportunities or a competitive edge. Vicarious liability is expressly presumed.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

By virtue of its control over SOEs, the Communist Party of China (CPC) is an omnipresent participant in the corporate enforcement arena. The CPC established the National Supervision Commission (NSC) in March 2018 under the Supervision Law 2018. It is China's new 'super graft agency' and enjoys a status close to the cabinet. It has absorbed and extended the investigative and enforcement powers of the CPC's Central Commission for Discipline Inspection. The NSC may detain individuals, interrogate them for up to six months, freeze assets, search premises with a warrant and seize evidence. Moreover, detainees are not entitled to legal advice as the NSC operates outside the purview of the Criminal Procedure Law of the People's Republic of China of 1979 (as amended) (the Criminal Procedure Law).

The NSC's jurisdiction focuses on corruption and bribery by individuals but it is likely that both SOEs and MNCs will get caught up in investigations initiated by the NSC, particularly given its ability to call on the services of other law enforcement agencies.

The NSC carries out investigations of suspected bribery by SOEs and state personnel before referring cases for potential criminal investigation or prosecution by the Ministry of Public Security, public security bureaux (PSBs), people's procuratorates and the Supreme People's Procuratorate. PSBs and people's procuratorates are organs of state and constitute the police and investigative arms, and the prosecution service, respectively.

PSBs investigate, via the economic crime investigation units set up within the bureaux, criminal bribery offences, fraud, other financial crimes, and crimes relating to food and drug safety. People's procuratorates, as prosecuting bodies, enjoy their own investigatory powers, but are primarily responsible for prosecutions. According to the Supervision Law, people's procuratorates will prosecute if they are of the opinion that the facts of a crime have been ascertained and the evidence is concrete and sufficient. The authorities have published no policies specifically relating to the prosecution of corporations, although there are thresholds for the investigation of corporates (see question 4).

Distinct from law enforcement, other bodies exercise investigative, disciplinary and regulatory powers over corporates. For example, the State Administration for Market Regulation (SAMR) investigates potential violations of the AUCL and sanctions civil bribery. It is not unusual for multiple agencies to be involved in a single matter. If relevant and within their jurisdiction, authorities do not generally refrain from pursuing matters simply because the corporate is under investigation by another domestic body.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

In practice, the authorities have considerable leeway in initiating investigations, both procedurally and substantively. The NSC in particular enjoys broad investigative powers, with no particular suspicion threshold stipulated in the Supervision Law.

The Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security have issued guidelines that prescribe minimum monetary thresholds for commencing investigations for certain financial crimes, including minimum thresholds for investigations of corporations.

The Criminal Procedure Law contains a general provision that investigative authorities should 'promptly examine the materials provided by a reporter, complainant or informant, or any voluntary confessions by any suspect'. After initial examination and preliminary investigation, if they consider there are facts indicating criminal liability, they should initiate a formal criminal investigation. The Criminal Procedure Law contains no other insight on the threshold of suspicion required to trigger a formal investigation.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Assuming that the investigating authority is properly authorised to issue the notice, it is unlikely that a person will have a valid ground to challenge a notice, given that the concept of privilege is not recognised under Chinese law. Challenges to procedural issues may be raised, but such issues can usually be resolved through government actions (e.g., issuance of an amended notice with proper authorisation). In addition, even if a person refuses to produce documents, the investigating authority has broad power to search and seize evidence during an investigation.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Whether an individual is granted any leniency or immunity for assisting with authorities is generally a matter left to the discretion of the authority. However, both the Law on Administrative Penalty and the Supervision Law (enacted in March 2018) contain provisions for more lenient penalties to be available when an individual has assisted or co-operated with authorities.

Article 27 of the Law on Administrative Penalty provides that lenient or reduced administrative punishments will be provided to those who have won credit in helping administrative organs investigate unlawful acts.

Similarly, Article 31 of the Supervision Law provides that the supervision organs may issue a recommendation for lenient punishment when a person actively co-operates with the authorities, takes active measures or otherwise renders significant assistance in cases involving matters of major national interest.

7 What are the top priorities for your country's law enforcement authorities?

Recent cases against corporations highlight corruption, fraud, product safety, tax evasion, money laundering and terrorism financing as the key areas of focus. As noted in question 1, there has been an increased focus on investigating potential economic crimes in certain sectors, such as the pharmaceutical, technology and the financial sectors.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

The Cybersecurity Law (CSL) is the key legislation regulating cybersecurity. It contains a set of cybersecurity obligations and requires the authorities to take action against companies and management in relation to cybersecurity-related failings. A key regime under the CSL is the Multi-Level Protection Scheme (MLPS). This requires each network operator to be assessed and designated a particular level of security obligations. The MLPS will be implemented through technical standards and a regulation that is currently being drafted by the Ministry of Public Security.

The penalties applicable in the case of a violation of the CSL include an order for rectification, warning, forfeiture of illegal income, fines, suspension of business, closure of website, withdrawal of operation permit or revocation of business licence. To date, most enforcement actions have focused on warnings and orders for rectification. However, with the MLPS regime being established, more enforcement actions are expected.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Cybercrime is regulated under the Criminal Law of the People's Republic of China of 1979 (as amended in 1997) (the Criminal Law), which punishes:

- illegal invasion or control of computer systems (or providing programs or tools for such);
- destruction of computer systems causing serious consequences;

- refusal to discharge cybersecurity protection obligations despite administrative orders, resulting in serious consequences;
- using information networks to commit certain crimes, such as fraud and the sale of drugs; and
- abetting others in committing cyber-related crimes.

These crimes are punishable by fines and imprisonment for up to seven years. China's law enforcement authorities have been focusing on infringement of personal data and intellectual property, cyberfraud, cybergambling, cyberpornography and online exam cheating. Law enforcement authorities receive many requests for assistance in cybercrime investigations from international agencies, such as Interpol, and counterparts overseas.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In general, the Criminal Law applies when either the act or the consequence of a crime occurs within China. Individuals who commit a criminal act are subject to the Criminal Law if they are located in China, regardless of their nationality, and Chinese nationals who commit crimes outside China are subject to the Criminal Law provided the punishment is more than three years' imprisonment. The Criminal Law applies to companies organised under Chinese law, including joint ventures, representative offices of non-Chinese enterprises and wholly foreign-owned enterprises.

In late 2018, China passed an amendment to the Criminal Procedure Law to allow judgment to be delivered in corruption cases when the defendant is absent. The amendment is designed to tackle cases in which suspects escape justice by hiding overseas. The amendment allows prosecutors to proceed with a case if evidence against the suspect is ample and the crime is clear.

The bribery of foreign public officials by individuals and entities was criminalised in 2011 through an amendment to the Criminal Law. This has not been prosecuted in practice.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

In practice, cross-border investigations involving conduct in China are typically triggered by the US authorities (the Department of Justice or the Securities and Exchange Commission). The principal challenge is how to deal with Chinese laws on issues such as data privacy, state secrets, trade secrets and the absence of privilege, while seeking to co-operate with US enforcement authorities. The movement of evidence from China is particularly problematic. The divergence in both procedural and substantive law in these areas means that what the US authorities expect from a corporate investigation, and what the corporate can do and provide within the purview of Chinese law, are often at odds. This in turn leads to tension between complying with Chinese law and demonstrating co-operation, which is necessary for leniency, deferred prosecution or a declination in the United States.

While challenges are most often encountered in the context of US cross-border investigations, similar tensions may be encountered in relation to other jurisdictions who may be investigating corporate conduct in China.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Chinese law does not expressly recognise the concept of double jeopardy or anything similar, even for domestic criminal proceedings. In fact, under the Criminal Procedure Law, even if a case has been closed, it can be retried if there is new evidence suggesting that the facts relied on in the original judgment or sentencing were incorrect. In practice, it is not uncommon for a defendant to become a suspect again in respect of the same allegations after a court has delivered a not-guilty verdict.

China is also unlikely to recognise the double jeopardy concept in international criminal enforcement actions. Under the Criminal Law, a person may be investigated and prosecuted in China even if he or she has already been tried in a foreign country. However, those who have received criminal punishment overseas may be exempted from punishment or receive a mitigated penalty. However, we are not aware of informal negotiation or co-operation to afford corporate defendants relief in the face of enforcement actions in multiple jurisdictions.

There is no system analogous to the US 'anti-piling on' policy.

13 Are 'global' settlements common in your country? What are the practical considerations?

We are not aware of any concluded global settlement involving China.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Decisions of foreign authorities may be influential for a number of reasons. They may draw the attention of the Chinese authorities to the matter. They may also serve to make the issue newsworthy and therefore exert political pressure on the Chinese authorities to escalate the matter themselves.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

China does not have a comprehensive sanctions programme in the same way as other jurisdictions, such as the United States. Rather, the legal basis for its sanctions programme is found in a patchwork of laws and regulations. The Foreign Trade Law authorises China to take corresponding measures against any country or region in response to discriminatory

measures. It also allows China to take action based on breaches of anti-monopoly or unfair competition laws. The Customs Law and the Regulations of the People's Republic of China on Import and Export Duties (through which China imposes customs duties) also form part of China's sanctions programme. The Ministry of Foreign Affairs issues circulars that serve as the legal basis for other organs at ministerial level to implement UN sanctions. Through the Ministry of Foreign Affairs, China also unilaterally threatens or imposes sanctions based on its foreign policy needs. For instance, in July 2019, China threatened to sanction US companies involved in selling arms to Taiwan.

China has released a draft of its Export Control Law, which seeks to bring China's export control system closer to other regimes. The draft Export Control Law introduces four categories of controlled items: dual-use goods; military items; nuclear items; and other goods, technologies, services and items that are related to national security. The draft Export Control Law also provides for the maintenance of a blacklist of foreign importers and end users that have been found to violate the law. According to the draft Export Control Law, China may adopt retaliatory measures against any country that imposes discriminatory export control measures against China.

On 1 June 2019, the Ministry of Commerce announced an Unreliable Entities List, which has been compared to the United States' Entity List. The Unreliable Entities List is understood to restrict the business of foreign companies in China that severely damage the legitimate interests of Chinese firms by not obeying market rules, violating contracts or blocking or cutting off their supply for non-commercial reasons. It is not known whether the Unreliable Entities List will be incorporated into the draft Export Control Law or whether it will continue as a stand-alone measure.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

China's approach to sanctions enforcement should be viewed in the context of its broader geopolitical status, particularly the ongoing trade war between the United States and China. Enforcement could increase in light of the draft Export Control Law and its possible incorporation of the Unreliable Entities List.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Generally no, unless this would be mutually beneficial.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

No.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Whistleblower reports (either internally to a compliance officer or colleague, or externally to a regulatory or enforcement agency) often trigger allegations of corporate misconduct. Internal audits may also identify misconduct. To a lesser extent, complaints by competitors, which may be channelled through media reports, can also cause allegations of misconduct to surface. Inspections by external bodies such as the SAMR or regulatory authorities may also flag issues.

Information gathering

21 Does your country have a data protection regime?

China's data privacy regime has been evolving quickly, conferring broader rights on data subjects and imposing ever more regulation on companies operating in China. The CSL, which came into force in June 2017, attempts to harmonise China's data privacy laws. Prior to the CSL, data privacy rights had been arranged in a patchwork of legislation (including the Criminal Law, the Civil Law and the Tort Law), and in industry-specific regulations (e.g., the banking, healthcare and securities sectors).

The CSL's data protection provisions cover any data that is generated, collected or processed in China by network operators – this covers both domestic companies and MNCs. Data collection must comply with relevant laws and regulations and be for a legitimate and necessary purpose. Consent of the data subject to data processing is required. The Personal Information Security Standards, which came into effect in May 2018, provide the first general good practice guide on data protection, which may serve as a reference for both users and the authorities.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The Civil Law protects the privacy rights and personal data of individuals, who can bring a civil law claim against the infringer in court. An illegal breach of personal data privacy rights could, in serious cases, give rise to criminal prosecution and penalties, including imprisonment and a fine. A breach of the CSL may trigger administrative penalties, including a fine, suspension of the business, closure of a website and revocation of an operation permit or business licence.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

Investigations should always be conducted in compliance with applicable data privacy legislation (see question 60). In recent years, the Chinese authorities have taken an aggressive approach to data privacy violations in the context of internal investigations. For example, as part of an internal investigation, China Auto Logistics collected data about its employees, which the employees subsequently reported to the police. A number of executives of the company resigned following the investigation and the company announced that its securities would be delisted from the NASDAQ stock market in August 2018. Data privacy laws

should therefore be borne in mind in the context of investigations and companies should handle relevant data with the utmost care when conducting or responding to an investigation.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Interception of employees' communications by an employer is restricted and must be conducted in accordance with the law.

Interception by employers of employees' communications on employees' personal property is generally prohibited unless explicitly permitted by the employees. It is important for an employer to make clear to employees that they should not have work-related communications on their personal devices, to avoid potential risks of leaks of confidential work-related information.

Interception of employees' communications on employers' devices or systems is possible, subject to compliance with cybersecurity and data protection laws and regulations. Employees need to be made aware that communications on their employer's devices or systems could be intercepted by their employer. This is usually dealt with at the onboarding stage. Additionally, prior consent from employees should be obtained for the collection, review, search, holding, processing and transfer of information and communications on employer devices or systems for employment-related reasons.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants and dawn raids are a common feature of law enforcement in China. Pursuant to the Criminal Procedure Law, a search warrant issued by a chief prosecutor of a people's procuratorate or the head of a PSB is normally required before conducting a search in a criminal investigation. However, in emergency situations, including when the person under investigation may conceal, destroy or transfer evidence of a crime, a search may be conducted without a search warrant.

The Supervision Law empowers the NSC to conduct broad searches and seizure with a warrant. The Criminal Law authorises investigators from people's procuratorates and PSBs to conduct wide searches and to seize property and documents found during a search to prove a crime. Other authorities (e.g., the SAMR and antitrust law enforcement authorities) may also conduct searches within the scope of their competence and functions.

Chinese law imposes few limitations on authorities executing search warrants other than the requirement that the search should be witnessed and recorded. Corporations subject to investigation may challenge the authorities' decisions or action during a search (e.g., restriction of personal freedom, sealing up, seizing or freezing of property) before the courts.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Privilege in the common law sense is not recognised under Chinese law. Authorities therefore have wide powers to seize documents and, in practice, may demand documents that would be protected from disclosure in other jurisdictions. There is no right to resist the disclosure of legal advice or other categories of evidence.

While lawyers owe their clients a duty of confidentiality, this does not assist if documents are sought directly from a client or a third party rather than the lawyer. Moreover, under the Lawyer's Law of the People's Republic of China, this duty of confidentiality does not apply to communications aimed at or involving criminal acts causing harm to state security, public security or persons and property. Additionally, this duty may be overridden in the context of investigations. The authorities have a general power to collect or obtain evidence from relevant entities and individuals concerned with a case pursuant to a search warrant or court order.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

There is no right to privilege over documents (see question 26). Article 52 of the Criminal Procedure Law explicitly prohibits a suspect from being compelled to give evidence to prove his or her own guilt. This protection was introduced in 2012. It is ambiguous as Article 52 only limits the measures interrogators can use to force interviewees to talk. They still have an obligation under the Criminal Procedure Law to answer truthfully all relevant questions put to them. Owing to its imprecise scope and an apparent continued enforcement of the previous law, which afforded no such protection, this right is likely to be of limited use in practice.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Under the Provisions of the People's Procuratorates on Reporting of Crimes 2009 (strengthened in 2014), whistleblowers who report crimes to the enforcement authorities are entitled to protection, anonymity and a right of appeal in the face of refusals to investigate. There is also a reward mechanism for whistleblowers who report crimes to people's procuratorates, and various other financial reward schemes are scattered in sector-specific regulations. The Criminal Procedure Law also contains several measures that protect the personal safety of witnesses giving evidence in legal proceedings and their families, including keeping personal information about witnesses confidential, and adopting protective measures so that the witnesses' appearance or voices are not made public.

An employee who is dismissed for whistleblowing would need to commence an action for wrongful dismissal against the employer, claiming either reinstatement or compensation. Retaliation by employers against whistleblowers in certain circumstances may constitute offences under the Criminal Law and Chinese labour laws. In such cases, the employee should report the matter to the people's procuratorate and the labour authority, as applicable.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Chinese labour laws are generally employee-friendly. In the course of an internal investigation, an employee must continue to be paid in accordance with his or her contract (salary and position are key terms that may only be altered with the mutual consent of the employer and the employee).

During an internal investigation, an employee may submit a dispute to the Labour Dispute Arbitration Commission for resolution. If the employee does not accept the arbitral award, the employee may generally institute court proceedings.

Officers and directors enjoy the same rights as employees. However, the employer may sue officers and directors in a civil action for breach of fiduciary duty separate from an employment claim. However, the employer cannot be compensated twice for the same damage.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

If an employee is subject to a criminal investigation by a prosecutor of a people's procuratorate, the employer may suspend the employment contract. If the employee is not convicted of a crime, he or she may ask for state compensation for lost salary and may request reinstatement. If the employee is convicted and sentenced for a crime, the employer may unilaterally terminate the employment on the sentencing date.

In general, as long as an employee continues to be paid his or her basic salary, the company can suspend the employee pending an investigation. As regards dismissal for refusing to participate in an internal investigation, an employee's contract cannot be terminated at will. An employer must have permissible legal grounds, such as a serious violation of company policy by the employee, or if his or her misconduct has caused material damage to the company.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

Generally, if an employee refuses to participate in an internal investigation, this is not of itself a sufficient ground for summary dismissal. In practice, terminations are generally agreed privately on the basis of a payment to the employee. Liability for wrongful dismissal is twice the statutory severance.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

This is likely to depend on the nature of the company. While investigations are not unusual, the management of a Chinese company is unlikely to conduct its investigation in such a

structured fashion. Being a domestic company, management and the company's lawyers are also likely to be less concerned about issues such as protecting privilege or procedures for transferring data and state secrets overseas. Such matters are likely to be of far less relevance. If, on the other hand, the company is an MNC, the China branch or its lawyers will generally prepare a document setting out the scope of the investigation, which is likely to include such issues.

The scope of any investigation plan will depend on the type and complexity of the issues being investigated, the level of detail needed to brief members of the board or management about the investigation, and the preferences of the company and professionals running the investigation. Generally, it will address who comprises the investigation team, the external lawyers or third-party experts (if any), and the objectives and scope of the investigation. The latter would cover who needs to be interviewed and the document types and date ranges to be searched (addressing privilege and dealing with state secrets and data transfers as appropriate).

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

China's culture is largely a collective, hierarchical one and it is likely that those within the company will report up internally. However, reporting externally is a different matter.

As part of the company's internal investigation, any duty to report the matter to law enforcement authorities or regulators (in the case of a regulated entity, see below) should be kept under review.

There is a general duty on individuals and entities under the Criminal Procedure Law to report suspected crimes to the PSB, the people's procuratorate or the court; however, there is no specific penalty for a failure to do so. Therefore, the provision lacks teeth and the obligation does not tend to be observed in practice.

If the company is a regulated entity, for example a financial institution, trading house, insurer or food and drug company, notification requirements are very likely to apply. If it is a domestic, non-regulated entity, it is not common practice that the company will report the issue externally.

In respect of MNCs operating in China, there may be more structured processes in place for reporting internally, as well as an awareness and culture of reporting externally. This may also be influenced by the approach of the lawyers representing the entity.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Under Article 54 of the Criminal Procedure Law, an investigating authority may request evidence from relevant entities or individuals. In practice, evidence collection might be accomplished by broad document seizure authorised under a seizure permit. However, it is also possible for an enforcement authority to issue notices for the provision of certain documents or data (especially when the person receiving the notice is not the direct target of the criminal investigation).

There are no strict rules regarding the preservation of documents or electronic data, or the issuing of litigation holds. However, intentional destruction or tampering with evidence is prohibited. Given that a domestic enforcement action could easily attract the attention of enforcement authorities in other countries, it is preferable that a proper litigation hold notification is issued and implemented.

The government is unlikely to allow the entity being investigated to propose its own custodians or search terms. Instead, it might ask the defendant to freeze all electronic data on the system and then conduct its own review of the data collected.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Privately owned companies and unlisted SOEs are generally not required to make public the existence of an internal investigation or contact from a law enforcement authority.

Under applicable securities laws, issuers and listed companies (including relevant SOEs) must observe their respective information disclosure obligations pursuant to applicable laws. Major investigations and litigation are generally required to be disclosed in annual and interim reports of listed companies. In addition, listed companies must generally immediately disclose any major event that may have a significant effect on the trading price of its securities.

36 How are internal investigations viewed by local enforcement bodies in your country?

Internal corporate investigations, particularly SOE audits, are common in China. What is quite unusual is self-reporting to local enforcement bodies on the back of an internal investigation. Usually, internal investigations identify remediation steps that are actioned by the company and this concludes the matter. The notion of self-reporting does not generally arise unless it is in the context of foreign enforcement bodies, and parallel reporting to Chinese law enforcement may then be considered. See questions 51 and 52.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

No. However, if the conduct in question is, or is likely to be, investigated in a common law jurisdiction, the company and its lawyers should conduct themselves in such a way as to maximise privilege.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

No concept of attorney–client privilege exists in China (see question 37). A lawyer owes a duty of confidentiality to his or her client, but this is not akin to legal privilege in the

common law sense. In any event, this duty of confidentiality does not apply to communications aimed at or involving criminal acts causing harm to state security, public security or persons and property. This is widely interpreted, rendering the scope of confidentiality protection limited in practice.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

No concept of attorney–client privilege exists in China.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

No concept of attorney–client privilege exists in China.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

No concept of attorney–client privilege exists in China.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

No concept of attorney–client privilege exists in China.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

No concept of attorney–client privilege exists in China.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

No concept of attorney–client privilege exists in China.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

No concept of attorney–client privilege exists in China.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes, this is common practice.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

No concept of attorney–client privilege exists in China.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There are no strict rules in China relating to the conduct of interviews (such as the requirement to give an *Upjohn* warning). However, the interviewer could be criticised for not explaining the situation and being transparent (e.g., if the investigation is likely to involve contentious labour law issues). Therefore, from a practical perspective, it is advisable to give something similar to an *Upjohn* warning.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Interviews will usually be conducted at the company's offices, with in-house counsel and external lawyers present. The interview usually involves a chronology covering employment history, the alleged events and the employee's recollections of the events. Assuming they are available, documents will be shown to the employee.

In general, the question of the employee's legal representation will turn on whether the investigation relates to an MNC or a domestic company. An MNC is likely to allow employees to have their own representation, from cultural and risk perspectives (potential exposure in another jurisdiction would militate in favour of allowing separate legal representation for the employee).

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Yes, see question 33. Under the Criminal Procedure Law, crimes should be reported, but this is not commonly observed in practice. Reporting of misconduct to regulators and to law enforcement authorities, as appropriate, will be mandatory in most regulated sectors in China.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting in China is often regarded as a confession; indeed, the terms are regularly used interchangeably in a way they are not in the West. The assessment of whether to self-report is generally driven by the risk that a third party may disclose the matter to the authorities. Usually, the risk of an individual disclosing the matter to Chinese law enforcement authorities is lower than in the West.

In practice, and where the matter raises potential liability overseas, a report is usually made to the relevant law enforcement authority in that jurisdiction before anything similar is done in China (e.g., for the purposes of leniency or co-operation credit). Disclosure to foreign law enforcement authorities generally raises the concern that the matter will become public. This in turn may prompt disclosure by the company to the Chinese authorities. Self-reporting is viewed by the Chinese authorities as being highly unusual.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

Self-reporting can be challenging in practice. Finding the right person to report to and documenting the report (e.g., for mitigation purposes) is not straightforward. Law enforcement officials may approach the concept of self-reporting with some doubt (see question 51), and may in turn be reluctant to sign documents or officiate the process. Moreover, it is very unusual in China to involve external lawyers when dealing with regulatory or criminal authorities before charges are laid, partly for reasons of face.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

It is possible to enter into a dialogue with the investigating authority to clarify the scope of evidence sought, or even to further limit the evidence. This dialogue can be conducted through formal or informal channels, with or without lawyers. However, the investigating authority may choose not to accommodate any such request.

54 Are ongoing authority investigations subject to challenge before the courts?

A person or company subject to investigation may bring administrative proceedings against an authority's decision or actions. Pending litigation, the authority's action (e.g., seizing or freezing property) is not usually suspended. In exceptional cases, where non-suspension would result in irretrievable damage or if the relevant administrative authority deems it necessary to suspend the action, the court may, upon request, order suspension of the alleged action. The amended Administrative Procedure Law lowered the threshold for bringing an administrative proceeding. However, from a practical perspective, the courts may lack sufficient muscle to deliver judgments without interference from government departments.

Aside from recourse before the courts, an individual may file a petition or complaint to PSBs and people's procuratorates against the unlawful exercise of certain powers in an investigation. These do not tend to be rigorously reviewed. In addition, Article 60 of the Supervision Law provides for certain acts of the NSC to be forwarded to a supervisory body for review within a month. It is too early to say whether and how challenges to the NSC's investigative powers will be addressed.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

The Chinese authorities are unlikely to limit the scope of their review in consideration of foreign laws. Indeed, since China does not recognise the concept of privilege, the potential scope of disclosure to the Chinese authorities is far broader than under a notice issued by the authorities of common law countries (see questions 26 and 27).

The company should seek to comply with each notice, ring-fencing and curtailing disclosure pursuant to applicable laws by asserting legal rights. Issues may arise in China in relation to the transfer of personal data, state secrets and trade secrets overseas. Any appraisal of notices received from another country should ensure that any data and documents are only transferred out of the country in accordance with the limited exceptions provided under Chinese law.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In practice, when a search is conducted and the information sought is located overseas, Chinese authorities have not generally expected companies to search outside mainland China and its Hong Kong and Macao special administrative regions (SARs). The authors are aware of a limited number of circumstances in which material on servers in Singapore has been sought and provided, but this is rare.

Technically, while investigating authorities may seek to impose such a requirement, they may not generally directly search and seize data overseas. Treaties on mutual legal assistance in criminal matters have been signed by China with 61 jurisdictions but these are of limited practical assistance in requiring a company to produce documents located overseas. In practice, the investigating authority might use other means (e.g., an administrative penalty) to seek to force a company to comply if the data located overseas is regarded as highly important.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

The scope of assistance under bilateral legal assistance agreements includes mutual assistance in taking evidence, executing search and seizure warrants, and producing documents. In this regard, people's procuratorates and PSBs do conduct inquiries into corruption-related matters in response to requests from overseas law enforcement organisations and judicial authorities, or vice versa. Most bilateral agreements on legal assistance contain provisions for tracing, restraining, confiscating, sharing or repatriating the proceeds of crime.

Currently, China's authorities co-operate with SAR enforcement authorities (Hong Kong's Independent Commission Against Corruption and the Macao Public Prosecution Office) in tackling cross-border corruption mainly through a mutual case assistance scheme and practice between the enforcement authorities on the mainland and in the Hong Kong and Macao SARs. In addition, the Supervision Law expressly encourages international co-operation and

states that the NSC will coordinate anti-corruption co-operation with relevant countries, regions and international organisations and implement anti-corruption international treaties.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

People's procuratorates or PSB investigators must keep the following information confidential: the identity of the person who makes the complaint; the identity of any suspects; the identity of any witnesses; and any state secrets, trade secrets and matters of personal privacy or personal information. These provisions are intended to contain dissemination of information to third parties. The Supervision Law expressly requires the NSC to keep state secrets, trade secrets and personal privacy confidential. Given the NSC's power to involve other authorities in its investigations, sharing other information with third parties should be expected.

In general terms, an investigation should be kept confidential. By disclosing matters about an investigation to a third party, a person may fall foul of Article 50 of the Law on Penalties for Administration of Public Security. This Article punishes those who obstruct a functionary of a state organ (which includes the various investigating bodies) from performing their duties.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

It is not typical for Chinese law enforcement authorities to request documents located overseas from a Chinese company (see question 56). If they do, and to comply would violate the laws of the other country, this should be explained. The Chinese authorities will generally respect this. Though this should not be necessary, the company could seek a legal opinion setting out how disclosure would violate such laws.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

At the end of 2018, China enacted a law governing how assistance is provided to foreign authorities and other bodies in criminal investigations. The International Criminal Judicial Assistance Law may serve as a blocking statute and restrict cross-border discovery of evidence. Institutions, organisations and individuals within China may not provide assistance to foreign countries without the consent of a competent authority, who may refuse on several grounds. In addition, the CSL attempts to harmonise rules on cross-border transfers of personal data. Draft regulations issued under the CSL indicate that personal and other important data can only be transferred offshore subject to a security assessment by the government authority. The government is currently drafting measures setting out the scope of security assessments. Since the CSL has significant implications for Chinese companies and MNCs operating in China, the new rules should be kept under review.

A related point concerns state secrets in the context of foreign notices or subpoenas. State secrets are defined very broadly. Therefore, the content of documents may be classified as a state secret under Chinese national security legislation. There is a risk that an investigation

of Chinese documents may implicate state secret issues. This will also affect the ability to transfer such documents overseas in response to a notice or subpoena.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Disclosure to the Chinese authorities is generally compelled in an investigation. While a producing party can assert that confidentiality attaches to the investigation conducted by the Chinese authority, whether that assertion will create an effective shield from disclosure will depend on the relevant Chinese and foreign laws. For example, pursuant to Chinese law, documents containing state secrets should not be disclosed to a third party.

Confidentiality requirements in China are very general and are unlikely to prevent the sharing of documents provided that disclosure is within the purview of Chinese law. Once documents have been shared with law enforcement authorities, a company cannot guarantee that they will not be shared with third parties. It is important for the company to assert its legal rights pursuant to the laws of the relevant jurisdictions so as to limit contagion issues.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

A corporate entity found guilty of misconduct will generally be sanctioned by a fine and confiscation of assets. The personnel in charge of the company and other personnel responsible for the crime may also face criminal liability (imprisonment, fines and confiscation of assets). In addition, individuals who have been convicted of corruption or bribery offences may also be disqualified from being directors or in senior management for five years.

As regards bribery offences, the April 2016 Judicial Interpretation to the Criminal Law introduced monetary thresholds for sentencing linked to the severity of the offence. For those in the private sector, individuals can be sentenced to up to 10 years for an offence of giving or offering a bribe and (technically) up to 15 years for receiving a bribe. Corporates committing bribery offences are liable on conviction to fines ranging from 100,000 yuan to twice the amount of the bribe.

For civil bribery offences under the AUCL, a corporate entity and its officers and employees may face administrative fines up to 3 million yuan, revocation of business licences and confiscation of illegal gains.

The Supervision Law expressly empowers the NSC to confiscate, recover or order restitution of ill-gotten gains. It should transfer such assets to the people's procuratorate to then prosecute in the usual way.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Government procurement is conducted by local government under the general guidelines set out in the Government Procurement Law. Serious illegal conduct (i.e., any conduct that results in criminal liability, revocation of business licence or large civil fines) within the previous three years should disqualify an entity from participating in government procurement under Article 22 of the Government Procurement Law. In addition, misconduct during government procurement (e.g., corrupt acts that result in a fine ranging from 0.5 per cent to 1 per cent of the procurement value) will also disqualify an entity from participating in future government procurement for a period of one to three years under Article 77 of the Government Procurement Law. Although there is no national registry of qualified government contractors, the government has maintained a publicly available list of suppliers subject to the debarment under Article 77 of the Government Procurement Law, and information regarding serious illegal conduct under Article 22 is generally accessible via company searches on relevant Chinese authorities' websites.

64 What do the authorities in your country take into account when fixing penalties?

Under the Criminal Law, the Chinese courts should take into account factors including the nature of the crime, circumstances relating to the criminal conduct and the damage caused to society. Circumstances relating to the criminal conduct include aggregating or mitigating factors, such as whether it is a first or repeat offence, or self-reporting. Additionally, the courts may exercise discretion in considering other circumstances, such as motive, the surrounding circumstances and whether there was any confession.

Regarding criminal bribery offences, both the ninth amendment to the Criminal Law (November 2015) and the April 2016 Judicial Interpretation provide clarification on the effects of self-reporting and co-operation. Generally, if the crimes are relatively minor or the offender has 'played a key role in investigating or solving a major case', self-reporting may mitigate or even exempt the offender from liability. Otherwise, offenders who self-report should be entitled to lenient treatment, but cannot expect to be exempted from liability. The Supervision Law also proposes leniency when a person surrenders or voluntarily confesses, actively co-operates with the authorities, takes active measures to disgorge ill-gotten gains or otherwise renders significant assistance in cases involving major national interests.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

No such settlement scheme exists in China.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

No such settlement scheme exists in China.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

No settlement scheme exists under Chinese law.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

It is not typical for Chinese law enforcement authorities to use external corporate compliance monitors as an enforcement tool.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Yes. However, this is rarely encountered given the domestic litigation environment, and the documents and files of the authorities would not be made available for a civil action. Also, authorities cannot share information classified as a state secret under the Chinese national security legislation. Procedurally, there are no class actions, derivative actions or analogous procedures to deal with broader issues of corporate fraud.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

At the investigatory stage, a confidentiality requirement is imposed through a general provision in the Criminal Procedure Law. By disclosing confidential matters about an investigation, a person may fall foul of Article 50 of the Law on Penalties for Administration of Public Security. See questions 27 and 58.

Once a case is before a court, the trial should technically be conducted with full public access unless state secrets, trade secrets or issues attracting privacy rights are implicated. Judges often take a very conservative approach, and access to the court by journalists and the general public is limited in practice. Although there is no general restriction on publicising a case during the trial process, this is rare in practice and parties to litigation are generally advised not to make public statements during trials.

Chinese media outlets are controlled by the state, for the most part. As such, investigations and trials involving SOEs, or broader public industry issues, are not fully reported in China (in contrast to overseas or Hong Kong media). On the other hand, the major private sector criminal investigation into GSK was reported in both China and overseas.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

The way in which corporate communications are managed will depend on the nature of the company (e.g., is it an SOE, a privately owned Chinese company, a listed company or an MNC with operations in China?). For the most part, it would be unusual for a public relations firm to be retained. However, this has occasionally been seen in high-profile matters involving MNCs or large multi-jurisdictional investigations involving the US authorities.

72 How is publicity managed when there are ongoing related proceedings?

Related proceedings may be in the public domain and therefore could attract more publicity. Generally, statements to the press about ongoing litigation should be limited, and contagion issues should be managed carefully throughout. Leaks to the press are not advisable; the parties should focus on the issues within the public court arena.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

There is generally no such mandatory disclosure requirement under corporate laws.

Under the PRC Security Law and related regulations, publicly listed companies are required to issue a market announcement of any major events that may materially affect the trading price of their shares. Although not specifically stated, settlement of criminal proceedings could constitute a major event, provided this materially affects the share price.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

There have been a number of changes recently that are designed to address both corporate and public misconduct. These include amendments to the AUCL and the introduction of both the Supervision Law and the International Criminal Judicial Assistance Law. There have also been administrative and structural changes to the enforcement of key legislation in this area, including the introduction of the NSC and the SAMR. The SAMR administers the AUCL and other antitrust legislation.

We anticipate that the focus of regulators and authorities will now shift to enforcement under these new laws, rather than further amendments. In fact, we have already seen a significant number of investigations commenced by these bodies.

That said, the recent focus on investigations in specific sectors may result in changes to the regulations or the publication of additional guidance to allow authorities to more closely monitor and regulate the activities in the pharmaceutical or technology space.

12

Colombia

Pamela Alarcón[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The highest-profile corporate investigations in Colombia are those regarding corruption in public contracts, and concessions in sectors such as infrastructure, health and public functions.

Criminal and administrative investigations that gain the highest profile are those related to illegal awards of public contracts, collusion and bribery to obtain public contracts and concessions, and breach of contract to the detriment of public finances and goods.

Odebrecht is currently the highest-profile investigation in Colombia, because of the amounts of money involved; the company has acknowledged paying US$11 million in bribes to government officials between 2009 and 2014 and US$6.5 million in relation to the contract for the Ruta del Sol 2 toll road concession.

As part of the criminal investigations, several other people, including a vice minister, a senator and the former president of Corficolombiana, have been sentenced for their involvement in the *Odebrecht* corruption case.

2 Outline the legal framework for corporate liability in your country.

One of the principles of Colombia's criminal law is *societas delinquere non potest*, whereby corporations cannot be held criminally liable. Nevertheless, it is possible for a corporation to be civilly liable in a criminal matter when the conduct of its employees or directors is related to their work or activities within the corporation, such as corruption (Colombian Criminal Procedure Code and Law 600, 2000). The Attorney General's Office enforces the sanctions and judges rule on the cases.

1 Pamela Alarcón is a partner at Philippi Prietocarrizosa Ferrero Du & Uría.

In terms of administrative liability concerning corrupt conduct, two principal authorities are in charge of imposing sanctions on corporations:

- The Superintendence of Companies imposes administrative sanctions on companies for transnational corruption conduct, under Law 1778, 2016. Additionally, when a sentence is executed against a legal representative or an administrator of a company located in Colombia or a branch of a foreign company, the Superintendence of Companies could impose a fine on the corporation of up to 200,000 times the minimum monthly wage.
- Antitrust practices such as collusion could also be liable to administrative sanctions on corporations as enforced by the Superintendence of Industry and Commerce (Law 256, 1996; Decree 2153, 1992; Law 1340, 2009).

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Administrative sanctions relating to transnational bribery are enforced by the Superintendence of Companies under Law 1778, 2016.

Other administrative sanctions linked with corrupt practices against free competition are enforced by the Superintendence of Industry and Commerce (Law 256, 1996; Decree 2153, 1992; Law 1340, 2009).

Civil sanctions relating to criminal activities are enforced by the Attorney General's Office, under the Criminal Procedure Code and Law 600, 2000.

Jurisdiction between the authorities is allocated depending on whether the case is civil, administrative or criminal. However, different authorities can pursue a corporation at the same time for the same conduct in the event that there has been an infringement of different laws or regulations.

Authorities may have internal policies or protocols relating to the prosecution of corporations; nevertheless, procedures are established in the laws, decrees and circulars.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The Attorney General's Office is obliged by law to initiate an investigation following a criminal complaint or receipt of information relating to a criminal complaint. There is no need to corroborate the information before the initiation of an investigation. However, prosecutors have the duty to verify the information and gather new evidence before the indictment.

In the same way, administrative authorities, such as superintendencies, have a broad discretion to initiate investigations.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Under Colombia's legal framework, natural and legal persons are encouraged to co-operate with the authorities. However, the lawfulness of a notice or subpoena may be challenged in any case with a constitutional action, such as a writ for protection of fundamental rights (*amparo*).

Depending on the law enforcement authority and the jurisdiction, and when the procedures permit it, ancillary claims or appeals against a subpoena or notice can be made before a fundamental guarantees judge.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Depending on the jurisdiction, co-operative agreements can be made with different authorities.

For some criminal matters, prosecutors may apply the principle of discretionary prosecution principle (Article 324, Criminal Code) or reach a settlement with natural persons who assist or co-operate with authorities.

Under Decree 1523, 2015, companies and natural persons involved in a business cartel may denounce its existence, confess their participation and provide evidence that will allow the authorities to sanction the other participants, and thus obtain total or partial leniency of a fine imposed by the Superintendence of Industry and Commerce for an infringement of free competition.

Additionally, Article 7 of Law 1778, 2016 establishes that sanctions for transnational bribery could be adjusted in consideration of criteria such as collaboration, acknowledgement or express acceptance of an offence.

7 What are the top priorities for your country's law enforcement authorities?

The top priorities for Colombia's law enforcement authorities are currently illegal drug trafficking, money laundering, financing of terrorism, corruption and antitrust practices.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Guidance on cybersecurity is established by the National Council of Economic and Social Policy (CONPES). Two strategy documents – CONPES 3701, 2011 and 3854, 2016 – set forth national cybersecurity policy guidelines with the aim of developing a national strategy to counteract the increase in computer threats that significantly affect the country. In this frame of reference, cybersecurity is defined as the capacity of the state to minimise the level of risk to its citizens and the degree to which they may be affected by cybernetic threats or incidents.

There is a broad national legal framework for cybersecurity relating to data protection, cybercrime and e-commerce, among others.

There are different guidelines for corporations regarding cybersecurity. For example, the Ministry of Information and Communications Technology – which is in charge of promoting the access, effective use and mass appropriation of information and communications technology – has issued guidance regarding the security and privacy of information, and for the assessment of digital security risk Assessment.

Finally, enforcement action in relation to companies' preparedness for and response to data breaches is taken by the Superintendence of Industry and Commerce. The majority of

such incidents relate to data breach protection. However, when breaches become felonies, criminal investigations may be initiated by the Attorney General's Office.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

With Law 1273, 2009, Colombia has included in the Criminal Code more than 10 crimes relating to cybercrime. Under Law 1928, 2018, Colombia adopted the Budapest Convention on Cybercrime.

Special units have been created within the national police service and in the Attorney General's Office to enforce cybercrime prevention and investigations.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Colombian criminal law has extraterritorial effect in six situations, as set out in Article 16 of the Colombian Criminal Code:

- if a person carries out any of the following acts in a foreign country:
  - crimes against the security of the Colombian state;
  - crimes against the constitutional system;
  - crimes against economic policy (excluding money laundering crimes);
  - crimes against public administration;
  - counterfeiting Colombian currency; or
  - financing terrorism;
- if a person working for the Colombian state is covered by international law immunity and perpetrates a crime in a foreign state;
- when a person working for the Colombian government is not covered by international law immunity but commits a crime other than those listed above, provided the perpetrator has not been convicted of that crime in the foreign country;
- if a Colombian person, except in relation to the aforementioned felonies, is in Colombian territory after committing a crime abroad, and when the sanction under Colombian criminal law is imprisonment of no less than two years, provided the perpetrator has not been convicted of that crime in the foreign country;
- if a foreigner (other than a person described above) is in a Colombian territory after committing a crime abroad that affects the Colombian state or a Colombian national, and when sanction under Colombian criminal law is imprisonment of no less than two years, provided the perpetrator has not been convicted of the crime abroad;
- if a foreign person perpetrates a crime abroad against another foreigner. Nevertheless, the crime must comply with the following conditions:
  - the offender must be in a Colombian territory;
  - Colombian criminal law sanctions the crime with imprisonment of no less than three years;
  - the crime is not political; and
  - extradition has not been granted.

Besides the aforementioned legislation, Colombian criminal law has extraterritorial effect for prosecuting cross-border bribery of a foreign public official in international transactions. This is regulated in Article 433 of the Colombian Criminal Code. (Note that Colombian criminal law only pursues individuals, not corporations.)

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The principal challenges that arise in cross-border investigations in Colombia are to:

- accomplish a constant and effective communication between the two countries' authorities that are in charge of the legal investigation and prosecution of the crimes;
- ensure that each country's authorities fully exchange useful information pertaining to criminal investigations;
- ensure effective co-operation between the countries involved, to carry out the legal investigation and prosecution of the felonies;
- identify (in the event that the countries with different laws regarding the same event) which legal framework is applicable;
- ensure that the legal authorities in the countries involved in cross-border investigations apply any precautionary measures requested by other states; and
- ensure that the legal authorities of the countries involved in cross-border investigations pursue assets relating to foreign felonies requested by other states.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Double jeopardy is established in Article 8 of the Colombian Criminal Code, specified as a prohibition of double criminality, in that no person can be charged more than once for the same criminal conduct, regardless of the name given to the conduct in other countries (provided that the core set of facts are the same).

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not legally binding nor are they common; however, Colombia has signed international treaties and co-operation agreements with various countries, including Peru, Brazil and Spain, for mutual assistance in pursuing certain crimes, such as cross-border bribery and corruption.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

According to the Colombian legal system in criminal matters, the decisions issued by a foreign authority abroad shall be legally binding for all judicial proposes. Therefore, the notion of prohibition of double criminality or double jeopardy, would also apply in this case.

However, this rule does not apply to decisions made abroad in connection with the following situations:

- when a Colombian national commits a crime abroad on a state-owned or state-operated ship or aircraft;
- when a person commits any of the following felonies in a foreign country:
  - crimes against the security of the Colombian state;
  - crimes against the constitutional system;
  - crimes against the economic policy (excluding money laundering);
  - crimes against public administration; or
  - counterfeiting Colombian currency; or
- if a person working for the Colombian state, who is covered by international law immunity, perpetrates the crime abroad.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

In an administrative case that falls under its jurisdiction, the Superintendence of Companies an impose the following administrative sanctions on a corporation for transnational corruption conduct (Law 1778, 2016): (1) disqualification from contracting with the Colombian government for up to 20 years; (2) a fine of up to 200,000 times the statutory monthly minimum wage; (3) publication in national newspapers, and on the website of the sanctioned legal entity, of an excerpt from the sanctioning administrative decision, for up to one year; (4) disqualification from receiving any type of incentive or subsidy from the government for five years.

Since Colombia does not have criminal liability for corporations, the sanctions on natural persons in a case of bribery could be imprisonment, a fine of between 66.66 and 150 times the statutory monthly minimum wage, or disqualification from contracting with the Colombian government for up to 20 years.

However, the disqualification from contracting with the Colombian government will extend to the corporation, its parent, its subordinates and the branches of foreign companies, with the exception of limited companies, if (1) the actions of the natural person involved in corruption crimes relate to the corporation's activities and (2) if a convicted person is an administrator, legal representative, member of the board of directors, or controlling partner or shareholder of the company.

Currently, numerous corruption investigations are being carrying out by different authorities; nevertheless, until now, only the Superintendence of Companies has imposed a significant fine on a corporation (4.6 billion Colombian pesos) in the framework of an agreement.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Since Law 1778, 2016 came into force, there has been an increase in enforcement activity relating to corruption investigations involving corporations and individuals; nonetheless, most of them are still under investigation, and therefore no sanctions have yet been applied.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Law 1573, 2012 promotes co-operation between the Colombian authorities and their counterparts in other countries for the purposes of enforcement of anti-corruption legislation. The Criminal Procedure Code and statutes such as Law 1778, 2016 also allow for international co-operation in investigations.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Colombia has not enacted any blocking legislation in relation to the sanctions measures of third countries. However, Colombia is a party to the United Nations Security Council Consolidated List of sanctions and it is common practice for reference to be made to the sanctions list compiled by the Office of Foreign Assets Control of the US Department of the Treasury.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct in Colombia most often come to light by means of media reports and criminal complaints. It has become more common that former employees of companies file complaints against it; therefore, whistleblowers are also relevant in allegations of misconduct. Note that collaboration agreements for whistleblowers are being vigorously enforced by the authorities.

Information gathering

21 Does your country have a data protection regime?

Individuals in Colombia have the constitutional right to be aware of, update and rectify the information about them in databases. This constitutional right is implemented by specific legislation on personal data protection and privacy – primarily by Law 1581, 2012, Decree 1377, 2013, Decree 1074, 2015 and certain additional implementing regulations.

There is also a separate specific regulation, primarily contained in Law 1266, 2008, that regulates the collection, use and transfer of financial information (i.e., credit, risk and banking information).

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The data protection regime is enforced by the Superintendence of Industry and Trade (hereinafter SIC), which has the power to initiate administrative investigations, *ex officio* or at the request of an interested third party. The SIC is active in its enforcement of the data protection regime, but the likelihood of an enforcement action will ultimately depend on the type of irregularity or infraction, and how it is brought to the SIC's attention. For any kind of violation of Colombian data protection regulations, the SIC may:

- impose sanctions (e.g., fines of up to 1.475 billion pesos, temporary suspension or cancellation of activities related to data processing); or
- order preventive measures (e.g., issue instructions to protect personal data).

The SIC may also co-operate with international data protection authorities when a foreign legal entity is violating the data protection rights of individuals located in Colombia.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

Under Colombian data protection regulations, any type of processing of personal data requires prior and informed consent. Moreover, personal data must be collected for specified, explicit and legitimate purposes. Thus, save for certain exceptions (e.g., public data, or information required by a government entity or in connection with judicial proceedings, among others), personal data may only be processed with prior consent and for the specific purposes for which it was collected.

Additionally, even in an internal investigation, individuals must be afforded all the rights granted by data protection laws.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

The interception of employees' communications may be legal as part of an internal audit or investigation. Nevertheless, the scope of that interception must remain restricted to corporate emails and other correspondence relating to company matters. Investigation of any other communications will be illegal without prior authorisation by a judge.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Yes. According to Articles 219 to 232 and 237 of the Criminal Procedure Code (Law 906, 2004), the following legal limitations apply to any authority executing a search warrant or a dawn raid:

- a written order from the prosecutor must exist, unless:
  - the owner or the holder of the property agrees with the authorities that the written order is not necessary;
  - the property is an open field, abandoned or in full public view; or
  - there is an emergency;
- the written order must be limited to a specific area of the property;
- the purpose of the written order is to gather evidence or to capture the possible liable person;
- a probable cause shall exist relating to the existence of evidence or that the possible liable person is inside the property; and
- a judge must study the dawn raid procedure within 24 hours after the competent authority has submitted its activity report, and confirm whether Colombian law has been respected.

If the above conditions are not met, the authority cannot admit any of the evidence that has been collected, and if a person has been captured, the authority must free him or her.

Furthermore, although there is no automatic redress, if the limitations are not observed, there may be legal consequences for the authority, such as for prevarication.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

During a dawn raid, a company or natural person can ask the authority in charge directly not to seize privileged material. If the authority nevertheless seizes this kind of material, the company or natural person can note this irregular situation in the dawn raids record.

Furthermore, the company or natural person whose privileged material has been seized can ask for a hearing to be held, at which a judge will study the specifics of the case and determine whether the material could be seized or not.

The authority must exclude from the investigation and process all privileged material that could be seized unlawfully.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

The general rule for an individual's testimony to be compelled is that anyone with knowledge about relevant facts that are investigated by the authority has the duty to testify. The person testifying must refer only to the truth, or otherwise be at risk of committing perjury. The

principal exceptions to this duty are the privilege of professional secrecy and the right against self-incrimination or incriminating a relative.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

In view of Colombia's history of civil war and the fight against illegal drugs and terrorism, there is a broad protection programme for informers, victims and public officials, mostly in connection with investigations relating to terrorism, illegal drugs, sexual harassment and violence. Nevertheless, in high-profile corruption cases too, whistleblowers may request protection.

The programme is under control of the Attorney General's Office and the National Protection Unit. There are also financial incentive schemes for whistleblowers, which are authorised by the government through the Ministry of Defence.

Further, Article 19 of Law 1778, 2016 establishes some benefits for whistleblowers in transnational corruption cases, such as total or partial exoneration of an administrative sanction.

The Superintendence of Companies also promotes the existence of whistleblower channels in corporations as good anti-corruption practice.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Colombian law does not limit employees' rights within the scope of internal or external investigations and there is no distinction between officers or directors for these purposes. Nonetheless, employees whose work requires monitoring and enforcing could be subject to internal company controls or have their employment agreement terminated if they are found to be in breach of their labour obligations.

To sanction an employee, a company must comply with the disciplinary procedure incorporated in both its employee handbook and the constitutional guidelines set forth in Ruling C-593 of 2014, which require the employer to notify the employee of:

- the date of the disciplinary procedure;
- the possibility of being accompanied by a co-worker during the procedure; and
- the misconduct that led to the procedure.

In addition, the employee has the right to:

- provide evidence and arguments that contradict the allegations made by the employer;
- evaluate the evidence submitted by the employer; and
- appeal any and all sanctions imposed.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Colombian law does not limit or differentiate rights for employees who are considered to have engaged in misconduct. A company may take disciplinary measures against such employees, following the disciplinary procedure set forth in its employee handbook and the constitutional guidelines.

Furthermore, employees whose job descriptions include additional ethical compliance obligations may have their employment agreement terminated for cause, in which case, the employee shall not be entitled to the legal severance payment.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

Yes. If this conduct has been included in the employment contract, handbook or company policy as a cause for termination of the employment agreement, the employer may terminate the labour relationship with cause.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Preparing a document setting out the terms of reference or investigatory scope before commencing an internal investigation will depend on a company's internal audit structure, its experience and the information available; however, it is common for internal auditors and members of a company's compliance department to do this.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There are no internal steps that companies are legally required to take. Nevertheless, it is important for the company to follow its own good practice policy. For instance, first, the company should conduct an internal investigation (using internal resources or hiring a third party specialist in auditing and risk consultancy) to enable it to gather information and documentation about the issue. Once the issue has been analysed and the compliance officer has assessed the risk, it is important to report the matter to the board. The compliance officer may consult an expert to gain an understanding of the possible consequences for the company, and thus be able to offer proper advice to the board regarding the best course of action to be taken. The board will decide whether to denounce the issue to the authorities, provided it is not mandatory under the Criminal Code.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Colombia's legal framework encourages individuals and corporations to co-operate with the authorities. Nevertheless, the lawfulness of a notice or subpoena may be challenged in any case with a constitutional action such as a writ for the protection of fundamental rights (*amparo*) or, in criminal case, before a fundamental guarantee judge.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

An internal investigation or contact from a law enforcement authority are confidential; therefore, there is no legal obligation to publicly disclose their existence.

Decree 2555, 2010 establishes that companies registered on the Colombian Stock Exchange must disclose 'relevant events'. Contact from a law enforcement authority could be interpreted as a relevant event if, for example, it could affect the share price or the company value.

36 How are internal investigations viewed by local enforcement bodies in your country?

The authorities always welcome internal investigations as a sign of co-operation. There are no requirements regarding the conduct or form of internal investigations, except for labour internal investigations, as discussed in question 29.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Attorney–client privilege may be claimed over communications or any kind of information exchanged between a lawyer and a client.

A company should have a professional relationship (i.e., a written contract) with external counsel and all communications or information shall refer to the matter of this relationship. Furthermore, the protected material shall specify that it is covered by attorney–client privilege.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

There is a general obligation for all professionals, including attorneys, to keep professional secrecy. Article 74 of the Colombian Constitution sets forth that professional secrecy is inviolable. This privilege protects the privacy as its underlying interest (Article 15, Colombian Constitution).

Attorneys must refuse to disclose or testify about a client's information. Lawyers cannot be compelled to testify against their clients. Nevertheless, lawyers can be excused from complying with this duty if they know that a crime has been, or is going to be, committed.

The holder of the attorney–client privilege is the client.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Although there is not a specific law that differentiates between in-house and external counsel regarding professional secrecy, currently it is considered that the privilege applies only to external counsel.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

The attorney–client privilege applies equally to advice sought from foreign lawyers in relation to an investigation in Colombia.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

The waiver of the attorney–client privilege is not necessarily considered a co-operative step. What triggers co-operative conduct is the fact that any person will share information about the investigation. In addition, there is not a specific context in which the privilege waiver is mandatory. However, there will be a lawyer will not be penalised if he or she contributes to stopping a crime from being committed.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Yes. As the client is the holder of the privilege, he or she can specify what part of the information he or she wishes to share and with what authority.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

If privilege has been waived on a limited basis in another country, it can be maintained in Colombia.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privileges does not exist in Colombia.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Yes. This could pertain to a new relationship protected with a new privilege, or part of the attorney–client privilege if the assistance relates to the same matter.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Colombia allows witnesses to be interviewed as part of an internal investigation.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Attorney–client privilege includes all the activities and information known by the attorney, if they relate to the attorney–client relationship. A company can claim attorney–client privilege in this situation.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

When interviewing with an employee or a third party in Colombia, the following steps are recommended:

- informing the interviewee:
  - who is the attorney's client;
  - that he or she has the right to have his or her own representation;
  - about the facts that are being investigated and the purpose of the interview;
  - that only the truth is expected and that possible falsehoods will be communicated to the authority;
  - if he or she is an employee, about the company's relevant internal policies;
- avoiding incriminating questions; and
- drawing up a record of the interview, which should include a signed declaration by the witness that the deposition was given voluntarily.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

An internal interview will typically include the following:

- explaining the nature of the investigation;
- asking questions to elicit personal information about the interviewee and his or her background;
- asking the witness about the facts being investigated;
- putting to the witness relevant documents found during the investigation – with prior authorisation from the client – and asking him or her about them; and
- listening to the witness's deposition.

The interview should be recorded and that record should be signed by the interviewee.

Employees may have their own legal representation.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Article 67 of the Criminal Procedure Code sets forth a general duty of reporting misconduct to law enforcement authorities. Nevertheless, in accordance with Article 441 of the Criminal Code, a penalty for non-compliance with this obligation will only be applicable when the said misconduct relates to genocide, enforced displacement, torture, enforced disappearance, homicide, kidnapping, terrorism, illicit enrichment, drug trafficking, money laundering, or any other misconduct that may affect sexual integrity.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

A company should self-report to law enforcement when any misconduct has been committed that jeopardises the company's legal activity, even if there is no legal obligation to do so.

In addition, the company should self-report in other countries when the misconduct could have a negative impact outside Colombia.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

An internal investigation regarding the misconduct should be carried out, and all relevant documents and information collected. The company should be advised about the legal consequences of the misconduct and the self-reporting. Depending on the case, the company should hire an attorney to ascertain the legal requirements for the self-report and its consequences.

The person or entity should co-operate with the competent authority during the investigation and ask the authorities to be admitted as a victim, provided this possibility is pertinent to the case.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Prior to filing charges, it is customary that the authorities enter into a dialogue with the company (except in a criminal investigation). The company should appear before the authority within the established notification period, be engaged in the case so that it can be informed, provide the necessary evidence and exercise its right to a defence.

The Colombian administrative sanctioning proceeding involves a preliminary investigation in which the authority determines whether there are reasons to open a formal investigation and to file charges. During the preliminary investigation, the authority is allowed to request the company's information, make inspections of the company's facilities, examine computers and obtain testimonies from the company's workers, officers and directors.

Throughout a preliminary investigation, some authorities, such as the Superintendence of Industry and Commerce, may allow the voluntary offering of information, and if the company offers warranties to the authority, its penalties may be reduced.

Overall, preliminary investigations are subject to confidentiality.

54 Are ongoing authority investigations subject to challenge before the courts?

Only a deciding administrative act can be appealed and challenged before the courts. A 'deciding administrative act' is defined as one that resolves the merits of the specific case and can produce a definitive legal effect. As such, authorities' decisions to initiate preliminary investigations and request evidence are not subject to judicial control in general.

Nevertheless, if within the investigation period there is a violation of the right of a fair proceeding, or if there is an infraction of a fundamental right, the company can file a constitutional injunction, which should be resolved by the court within 10 days.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

There is no standard practice as to how a company should act in this situation. The existence of a foreign investigation does not create effects to an investigation in Colombia per se. Recently, Colombian and foreign authorities have engaged in joint investigations in administrative matters. Colombian authorities are not obliged to follow foreign decisions, although in many cases they can be directly recognised in Colombia or through special proceedings.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

If a notice or subpoena from the authorities in Colombia seeks production of material relating to a particular matter that crosses borders, the company must search for and produce the documents in other countries to satisfy the request, unless it is impossible under the laws of the foreign country to obtain or reveal such information. The General Procedural Code establishes that when it is easier for one party to the process to prove certain facts, that party has the burden of providing the material to the authority. When the documents are in another language, they should be translated by an official translator and sent to the Ministry of Foreign Affairs for legalisation and apostilles as required by the relevant countries involved.

The costs of the translation and the time taken for the Ministry of Foreign Affairs to legalise the translation of the documents may be considered as difficulties.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Law enforcement in Colombia may share information or investigative materials with law enforcement in other countries, depending on the authority that is requesting the information.

Recently Colombia has become a member of the Organisation for Economic Co-operation and Development (OECD), which has led to Colombia signing different types of agreements for the exchange of information with international authorities, mostly concerning tax requirements compliance.

There is frequently an exchange of information with international authorities when the matter concerns trust, financial, criminal and corporate authorities.

Framework for co-operation with foreign authorities in Colombia

- Foreign Account Tax Compliance Act
- Foreign Corrupt Practices Act
- American Convention Against Corruption
- UN Convention Against Corruption
- OECD Anti-Bribery Convention
- Basel Committee (Basel III: International Regulatory Framework for banks)
- Law 1474, 2011
- Law 1712, 2014
- Law 1778, 2016
- Organic Statute of the Financial System
- Decree 1848, 2016
- Circular Externa 100-00005 of the Superintendence of Companies
- Decree 950, 1995

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

The enforcement authorities in Colombia should act according to the legal requirements regarding retention and secrecy for any type of information relating to fundamental and constitutional assets, especially when there is an ongoing judicial proceeding. Individuals can also request certain authorities (antitrust, financial, corporate and tax) to grant special confidentiality to the information disclosed during an investigation.

Concerning commercial companies, an authority is only allowed to order the disclosure of commercial books and papers for the following purposes:

- appraisal of taxes;
- surveillance of credit institutions, commercial companies and institutions of common utility;
- investigation of crimes; and
- bankruptcy and liquidation of companies in both cases and of successions in the latter.

There may be partial disclosure of commercial books in a situation other than as listed above, and the authority can only examine what is related to the specific litigation.

The disciplinary code for public authorities contains a ban on allowing access to records, documents or information by unauthorised persons during and after an investigation.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

A company that has received such a request should oppose the release of information establishing that the production of the content of the documents would violate the law in the other country. In this event, it is important that the company obtains a legal opinion with the translation of the support regulations, explaining why it is impossible under law to obtain, furnish or reveal that information.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

- Law 1581, 2012 establishes that any person who intervenes in the management of personal data is obliged to secure the confidentiality of that information.
- Decree 2153, 1992 establishes that natural or legal persons subject to Superintendence of Industry and Commerce investigations may request that any information regarding business secrecy, or information that is to be supplied during the investigation and the administrative process, be kept confidential. The company should paste a non-confidential summary of the matters included in the document on top of the privileged document. If the authority fails to meet this request, it is liable to disciplinary penalties.
- Law 1712, 2014 establishes that anyone can appeal a request for information when it involves commercial, industrial or professional secrets.

All information subject to investigation that is determined by its owners to be confidential cannot be accessed by third parties other than those who are part of the relevant judicial process.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

There is a potential risk relating to how the competent authority may interpret the behaviour of a company with regard to the compelled production of material. Nevertheless, that interpretation is not a substantive merit against the party that produces material. Private persons can also request certain authorities (antitrust, financial, corporate and tax) to grant special confidentiality to the information disclosed during an investigation.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Penalties under the Criminal Code that directors, officers or employees may face for misconduct in Colombia (depending on the crime) include:

- imprisonment;
- fines;

- seizure of goods and instruments used in committing the misconduct;
- disgorgement;
- forfeiture; or
- disqualification – for up to 20 years – from participating, directly or through a representative, in public contracting procedures such as public bids and government contracts.

Under the Criminal Procedure Code and Criminal Code, companies will be subject to a civil sanction that consists of paying for all the damage caused by the misconduct of their employees or directors, fines and disqualification from contracting with the government for up to 20 years.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

This does not apply in Colombia.

64 What do the authorities in your country take into account when fixing penalties?

When fixing penalties in transnational corruption cases, the Colombian authorities may consider a graded series of criteria for sanctions (Article 7, Law 1778, 2016), based on the following:

- the economic benefit obtained or intended by the offender by his or her conduct;
- the greater or lesser capital capacity of the offender;
- the repetition of behaviour;
- the resistance, refusal or obstruction to the investigative or supervisory action and the procedural conduct of the offender being investigated;
- the use of means or of the person interposed to hide the infraction, the specific benefits or money, the goods or services susceptible to economic valuation, or any benefit or utility, offered or delivered to a national or foreign public official, or any of the effects of the infraction;
- the recognition or express acceptance of the infraction before the decree of evidence;
- the existence and compliance of transparency and business ethics programmes or anti-corruption mechanisms within the company, in accordance with the provisions of Article 23 of Law 1779, 2016;
- the degree of compliance with precautionary measures;
- if an appropriate due diligence process has been carried out, prior to a merger, spin-off, reorganisation or acquisition of control process in which the company committing the infraction is involved; and
- if the authorities responsible for sanctioning commission of behaviours set forth in Article 2 of Law 1778, 2016 by employees, legal representative or shareholders, have been informed in accordance with the provisions of Article 19 of Law 1778, 2016.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Under Law 1778, 2016 (administrative liability of legal entities for acts of transnational corruption), non-prosecution or deferred prosecution agreements are not available in Colombia for corporations.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Under Law 1778, 2016 (administrative liability of legal entities for acts of transnational corruption), Colombia does not provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Under Law 1778, 2016, settlements with law enforcement authorities cannot be reached through agreement or negotiation. Although Law 1778 allows the authority to grant benefits in exchange for effective collaboration, the process for obtaining those benefits is not a negotiation but rather consists of filing a request with admissions of wrongdoing and supporting evidence for the same, and the authority will unilaterally determine the effectiveness of the alleged collaboration and make its own decision.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Law enforcement authorities in Colombia do not use external compliance monitors as an enforcement tool.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

No. Access to Law 1778 files is very restricted.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Under Colombia's Criminal Procedure Code (which applies only to natural persons), preliminary investigations undertaken by the prosecutor are classified. Therefore, information relating to the case will not be made public until the indictment. The Criminal Procedure

Code provides that all hearings must be public. However, judges may make some exceptions in relation to the publicity of certain criminal hearings.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common for companies to use a public relations (PR) firm to manage a corporate crisis, and larger companies will have their own PR and communications department. In either situation, it is also common for companies to hire criminal and compliance lawyers to work on the matter with their communications team.

72 How is publicity managed when there are ongoing related proceedings?

Ongoing proceedings are confidential until the indictment hearing. However, the media are always interested in high-profile cases, and will therefore gather confidential information, which is usually provided by the parties or authorities involved in the case.

When trials begin – since they are open to the public – it is common for the media to attend high-profile cases.

It is also common for individuals or companies to use the media to expose their case arguments to generate positive public opinion and to try to put pressure on the authorities.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Agreements may be confidential; thus, it depends on the kind of agreement that has been reached.

However, an excerpt from the sanctioning administrative decision sentence for transnational corruption will be published in newspapers and on the website of the sanctioned legal entity for a maximum of one year.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

During the next two legislative periods, we expect to see key legislative changes such as the approval of a law regarding criminal liability of corporations, as has been suggested and requested by the OECD. Therefore, compliance programmes will also be more regulated and enforced by different authorities.

13

France

Stéphane de Navacelle, Sandrine dos Santos, Julie Zorrilla and Clémentine Duverne[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The year 2019 marks a new era in the implementation of anti-corruption and financial crime measures in France. The *UBS* decision notably shows that the French authorities – and the National Financial Prosecutor (PNF) in particular – intend to adopt a more hard-line approach that has a noticeable effect on companies that violate French law. UBS, which chose to stand trial rather than settle through the French equivalent of a deferred prosecution agreement (a CJIP), was convicted on 20 February 2019 and ordered to pay a €3.7 billion fine and €800 million in damages to the French state for unauthorised banking solicitation, aggravated tax fraud and money laundering – the highest sentence to date imposed on a company for these offences. The choice to leave it to the courts, resulting in a considerably higher payout, has raised the question of the judicial strategy that prosecuted companies should adopt in such cases. Some have concluded that recourse to a CJIP would have been beneficial, while others await the decision of the appeal court, arguing that UBS has strong judicial arguments in defence.

Following the introduction of the CJIP, the French authorities clearly defined the first sets of rules: the Anti-Corruption Agency (AFA) and the PNF have published guidelines detailing the criteria to be taken into account when concluding a CJIP and assessing the fine.

A new CJIP has been signed between the PNF and Google following the failure by Google Ireland Ltd to subscribe to declarations to corporate income tax for the tax years 2011 to

1 Stéphane de Navacelle is a partner and Sandrine dos Santos, Julie Zorrilla and Clémentine Duverne are counsel at Navacelle.

2014. In this CJIP in the area of tax fraud, the PNF acted jointly with the tax authorities, which also entered into an agreement with Google regarding tax matters.

Another CJIP is pending with Airbus, which is currently under investigation. Since 2016, the aircraft manufacturer has been co-operating with the PNF and the UK's Serious Fraud Office in connection with allegations of corruption. The US Department of Justice (DOJ) subsequently joined the French–English investigation pool on a regulatory aspect: Airbus is alleged to have repeatedly omitted certain statements to the US authorities regarding the sale of weapons. This case is a renewed illustration of the tendency for international coordination between foreign authorities prosecuting the same facts. It is yet to be determined whether the prosecution pool will take the *Société Générale* case as an example case and coordinate a multi-jurisdictional settlement.

2 Outline the legal framework for corporate liability in your country.

Corporations can be held liable on both civil and criminal grounds. Corporate criminal liability is limited to 'offences committed on [companies'] account by their organs or representatives', namely for actions committed by persons who exercise direction, administration, management or control functions, or by persons who act on behalf of an identified delegation of power that meets specific criteria. Thus, corporate liability does not exclude individual liability.

From 2006, a new trend in case law appeared, by which the Criminal Division of the French Supreme Court (the Court of Cassation) found corporations liable without identifying an organ or representative, relying instead on facts that reflect an endorsement by company management. The Criminal Division has nevertheless reiterated that corporate criminal liability implies the identification of an organ or a representative.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Enforcement authorities include judicial and administrative authorities. For the most part, jurisdiction between the authorities is based on subject matter, with numerous opportunities for co-operation – and competition – between authorities.

Each superior court has jurisdiction over offences committed within its territory or based on the location of headquarters. Specialised interregional courts have jurisdiction over economic and financial matters of some importance or complexity and whose scope involves several jurisdictions. Some particular fields fall within the scope of specialised sections of the prosecution authorities in Paris; for example, terrorism, war crimes and human rights, health and safety, and the environment. The aforementioned PNF was created in 2013 to deal with breaches of probity, public finance and proper functioning of the financial market.

Alongside judicial authorities, the main administrative authorities with jurisdiction over corporations are the French financial markets authority (the AMF, which regulates the integrity of financial markets, ensuring investor protection and information, and preventing market abuse), the Competition Authority (which conducts sector enquiries, antitrust activities, merger control, and publishes opinions and recommendations), the French supervisory and resolution authority (the ACPR, which investigates wrongdoing, issues warnings

and sanctions French banks), the tax authority within the Ministry of Finance and the AFA (which controls, sanctions and monitors the implementation of anticorruption programmes by companies to which the Sapin II Law applies).

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

In respect of criminal offences, there is no minimum standard for a prosecutor to request enquiries to be carried out; prosecutorial discretion is considerable. In practice, investigations are opened after a complaint, self-report or *flagrante delicto*. If the matter is particularly complex, prosecutors may turn it over to an independent investigating magistrate to carry out a comprehensive investigation into the facts and give an opinion as to guilt. Investigating magistrates can also be required to investigate pursuant to a specific complaint filed by alleged victims, including, under specific conditions, non-government organisations.

Investigations can also stem from authorities' detection of suspicious activities within their material jurisdiction (e.g., if mandated by a foreign authority, responding to a report from a whistleblower or an alert triggered by the anti-money laundering branch of the Ministry of Finance (TRACFIN), or owing to a legal obligation to support facts that may constitute a criminal offence).

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Although exceptions do apply (e.g., the AFA), it is unlikely that an enforcement authority would use a notice or subpoena to collect documents or data. There is little ground for challenging such a request if it is within the scope of the authority's prerogatives and respects the legal requirements (see question 25). The company may argue against communicating data and documents that are covered by attorney–client privilege or medical secrecy, for instance.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

As such, there is no co-operative agreement that grants immunity or leniency for individuals. At the Société Générale CJIP (SG CJIP) certification hearing, Mrs Houlette, former president of the PNF, stressed that the company's co-operation had been taken into account in determining the penalty. The provisions of the CJIP do not create incentives for legal representatives to report misconduct as they remain personally liable for their actions during the performance of their work and the CJIP will only benefit the company. Similarly, whistleblower status does not provide for situations in which the person would agree to reveal his or her actions either. However, the guidelines enacted by the PNF regarding CJIPs expressly encourage the co-operation of legal persons to be eligible for the procedure and minimise the amount of any fine imposed.

7 What are the top priorities for your country's law enforcement authorities?

The two main priorities for enforcement authorities are tax evasion – for individuals and corporations – and corruption. Since it was created, the PNF has aggressively moved to fight

tax evasion, including in instances when the tax authorities themselves have decided not to impose sanctions, by relying on money-laundering offences. The PNF's ability to prosecute tax evasion has been extended by reducing the power of control and appreciation of the Ministry of Economy in this area.

The PNF currently has more than 240 open probity offences cases, of which 10 per cent involve international corruption. The Sapin II Law created the AFA – headed by a senior former investigating magistrate – which has carried out many audits of compliance programmes and, where a suspicion of crime is identified, referred the facts to the PNF.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Cybersecurity is a national priority in France. During the past 10 years, France has adopted a comprehensive framework at different levels to address the specific issues of cybersecurity: the central office for the fight against crimes linked to information and communication technologies within the National Police Office, the centre for the fight against digital crimes within the National Gendarmerie and the brigade for the investigation of information technology fraud within the Paris Prefecture. The National Information Systems Security Agency (ANSSI), created in 2009, is the national authority in the area of cyber-defence and network and information security. ANNSI's missions target government departments and public services, businesses and operators of vital importance, and aims to provide a proactive response to cybersecurity issues.

At the European level, a Regulation was adopted on 17 April 2019 on the European Union Agency for Cybersecurity (ENISA) and on information and communications technology cybersecurity certification (the Cybersecurity Act), giving ENISA a permanent mandate while strengthening its role and establishing an EU framework for cybersecurity certification.

As regards the enforcement of cybersecurity-related failings, when it comes to data protection, a failure to implement cybersecurity measures is an administrative offence, subject to administrative fines and civil liability (see question 22). Further, pursuant to the Law on Military Programming dated 26 February 2018, those with the status of 'operators of vital importance' have an obligation to implement a cybersecurity framework. Failure to comply is sanctioned by the French Criminal Code.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The legal framework for tackling cybercrime in France has grown steadily in recent years. Most of the tools used to regulate cybercrime are inspired by the Budapest Convention signed by the European Council on 23 November 2001. The French Criminal Code penalises cybercrimes relating to offences such has hacking and denial-of-service attack, and the French Code of Intellectual Property further sanctions phishing and possession or use of hardware used to commit cybercrime. These offences are punishable by imprisonment and fines of up to €375,000.

In addition, French law provides for an extraterritorial application of its provisions since a cyber offence is deemed to have been committed in France (i.e., committed through an e-communication network to the detriment of a person in France or a company with its registered office in France). The implementation of cybercrime regulations is coordinated by the Ministry of the Interior, in collaboration with the ANSSI and dedicated police services.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Criminal law can have an extraterritorial effect, based on the nationality of the perpetrator or the victim. It is applicable to any crime committed by a French national outside French territory. It is also applicable to a misdemeanour (*délit*) committed by French nationals outside French territory if the conduct is punishable under the legislation of the country in which it was committed (double criminality). French criminal law also applies to any felony, and to any misdemeanour punishable by imprisonment, committed by a French or foreign national outside French territory when the victim is a French national. The extraterritorial effect of French criminal law can also apply when an element constituting the offence takes place on French soil.

The extraterritorial reach of French criminal law can also apply in other limited circumstances, for instance when fundamental interests of the nation, diplomatic or consular premises are targeted. The Sapin II Law extends the extraterritorial effect of criminal law for corruption and influence peddling offences involving non-French perpetrators. French criminal law applies to acts of corruption or influence peddling committed abroad by a person carrying out all or part of their economic activity in the French territory.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

To a large extent, pressure to increase enforcement of international financial and corruption issues comes from the United States, and co-operation with the United States usually works well in those matters, despite regular tensions and the overall impression that US prosecutions are, at least in part, carried out in support of US industry. Co-operation with other EU Member States is generally smooth.

Concern arises from the blocking statute that applies when a foreign authority is involved. The purpose of the statute is to prohibit compelled communication of virtually any information of commercial value without some involvement of French authorities. It carries both a fine and a prison term for violations. Appropriate contact with the French authorities that have been taking the lead in explaining its legitimacy, should mitigate risks – the AFA is tasked with ensuring observance of the French blocking statute, in the context of corporate compliance programme obligations imposed on French companies by foreign authorities.

EU-wide data protection and privacy rules are enforced by the French Data Protection Authority (CNIL), and the right of privacy of individual employees and the management of personal information should be properly addressed. The EU's General Data Protection

Regulation (GDPR), adopted in France on 20 June 2018, has introduced new rules on communication of personal data to foreign authorities and requires, pursuant to Article 48 of the GDPR, without prejudice to any other grounds for cross-border transfers, that any transfer of personal data be based on international conventions such as mutual legal assistance treaties. Although burdensome, both can be dealt with effectively by addressing the privacy issue as a firm policy and complying with data protection rules.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The principle of double jeopardy is enshrined in Article 14.7 of the International Covenant on Civil and Political Rights, Article 50 of the Charter of Fundamental Rights of the European Union and Article 4 of Protocol No. 7 to the European Convention on Human Rights.

However, the French state has made an exception in the interpretation of Article 4 of Protocol No. 7, limiting the application of the rule to offences falling within the jurisdiction of courts ruling in criminal matters. On 11 September 2019, the Court of Cassation confirmed this restriction, refusing to consider that previous tax sanctions fell into the scope of the previous criminal sanctions authorising the application of the double jeopardy principle.

Another exception is provided by French criminal law, which states that there is no extra-territorial application of the double jeopardy principle.

On 14 March 2018, in a decision regarding the Oil-for-Food Programme, the Court of Cassation confirmed that Article 14.7 of the UN International Covenant on Civil and Political Rights applies only when both proceedings are initiated in the territory of the same state, and refused consequently to apply the double jeopardy provision to a US deferred prosecution agreement.

The European Court of Human Rights (ECHR) adopted a similar position on the *ne bis in idem* principle in the *Krombach* case. The applicant argued that the German decision to drop charges prevented France from prosecuting him for the exact same facts. This indicates that a foreign decision does not automatically have res judicata in another state, in line with recent French Court of Cassation decisions on the issue.

Although this appreciation by French case law and the fact that there is no equivalent to the US 'anti-piling on' policy in the current French legal landscape, that situation may change. Indeed, on 6 June 2019, France was convicted by the ECHR for violation of the *ne bis in idem* principle (*Nodet v. France*, Case No. 47342/14). The case involved a double penalty from the AMF and the criminal courts for market offences. The ECHR calls France to encourage the various authorities to ensure that each procedure is duly considered and that the overall amount of all penalties is proportionate.

13 Are 'global' settlements common in your country? What are the practical considerations?

Multiple authorities often investigate the same facts at the same time. There is no particular procedure for global settlements as relationships vary from co-operation to competition and sometimes lead to a race to a decision. A prior sanction or decision on the same facts will be taken into account by the other authorities involved. However, the CJIP agreed with Société Générale in 2018 (the SG CJIP) demonstrates an intent for stronger co-operation between authorities in the coming years (see question 14).

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

See question 12.

If a foreign court decision could be recognised by the French jurisdiction, the French authorities could decide to open their own investigation or to send the case before the French tribunals. However, the emerging trend is towards co-operation between French and foreign authorities. Efforts to co-operate with foreign authorities arise in the SG CJIP, for instance, although the US authorities were the first to open an investigation, as early as 2014. The PNF started working with the DOJ, reciprocally communicating details of the investigation on account of the mutual legal assistance treaty. It was determined that the fine would be divided equally between the DOJ and the PNF and the monitoring would be carried out by the AFA.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

The implementation of economic sanctions in France is essentially part of UN sanctions policy and the EU Common Foreign and Security Policy. Restrictive measures (such as asset freezes, embargos, commercial restrictions) are enforced by a European Council decision supported by EU Regulations and are directly binding on EU Member States. Unilateral measures can also be implemented by national decree or order. The sanctions may target governments of foreign countries, non-government entities and individuals. France's Ministry of Europe and Foreign Affairs oversees the implementation of any sanction decided at European level and is assisted by several ministries. On 17 May 2019, the Council of the European Union extended the economic sanctions against the Syrian government until June 2020, as the repression of Syria's civilian population continues. France officially acknowledged this extension by a decree dated 13 June 2019. The sanctions currently in place against Syria include restrictions on certain investments, a freeze of assets and an oil embargo. As regards the latter, the company LafargeHolcim has been prosecuted in France for violation of this embargo.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Economic sanctions are an instrument of France's foreign policy and, as an EU Member State, it follows decisions laid down by the European Union. Nevertheless, autonomous

measures can also be taken by each Member State. During the past few years, there has been an increase in measures to fight terrorism financing. For that purpose, the French Monetary and Financial Code entitles the Minister of Economy to order the freezing of assets belonging to individuals or legal entities who commit, or attempt to commit, terrorist acts, or who facilitate or participate in such acts (Articles L 561 and L 562). The French Directorate-General of the Treasury, which is the authority in charge of economic sanctions, published (on 17 June 2019) the updated version of the Guidelines drafted with the ACPR on the implementation of French economic sanctions.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

As part of a multilateral decision system, economic sanctions shall result from a collective implementation and co-operation. Nevertheless, there is a lack of precedent relating to implementation of sanctions in French law, and the *LafargeHolcim* case might create the first guidance if it goes to trial. In addition, there is still no general provision to criminalise the violation of economic sanctions, although a bill for this purpose was considered by the French Parliament in 2016.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

On 22 November 1996, in response to extraterritorial legislation in force at the time against Cuba, Iran and Libya, the European Commission adopted Council Regulation (EC) No. 2271/96 protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (the Blocking Regulation). This Regulation is directly enforceable in France. The measure forbids EU citizens from complying with third-country extraterritorial sanctions unless exceptionally authorised to do so by the European Commission (as set forth in Commission Implementing Regulation (EU) 2018/1101). On 6 June 2018, the Blocking Regulation was updated by the European Commission (Council Regulation (EC) No. 2271/96), adding to its scope the extraterritorial sanctions that the United States reimposed on Iran in August 2018.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Although the Blocking Regulation sanctions EU companies that would comply with third-country sanctions, the measure has much more of a symbolic effect than an economic one. It has only been applied in 1998 in the context of a complaint filed by the European Communities before the World Trade Organization. As regards the US sanctions on Iran, experts are sceptical about how far Europe will ultimately go to enforce such a rule. It could also prove difficult to enforce, in part because of the international banking system and the significance of the United States in international financial markets.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Whistleblowers are an increasingly common source of disclosure of misconduct within corporations (see question 28).

As some specific professions – including financial institutions – are required to report any suspicious activity to TRACFIN, anti-money laundering reports have generated several high-profile cases.

The Sapin II compliance requirement is likely to create a new compliance culture. The transitional phase is likely to generate its share of new matters.

Extensive freedom of the press and protection from disclosure of journalists' sources have led mostly web-based media to reveal facts resulting in prosecution of key political figures in recent years.

Under specific conditions, non-government organisations (NGOs) can initiate criminal procedures. Several landmark corruption investigations have been initiated by NGOs in recent years. For instance, in 2016, the NGO Sherpa filed a complaint against the cement group LafargeHolcim for alleged terrorist financing in Syria. In 2007, the Sherpa initiated criminal proceedings by a joint complaint with Transparency International France on charges of ill-gotten goods against the son of the president of Equatorial Guinea.

Information gathering

21 Does your country have a data protection regime?

France adopted a data protection regime in 1978 with the Law on Information Technology, Data Files and Civil Liberties. Legislation has been amended to integrate the GDPR in France's internal legislative framework. Law No. 2018-493, which was passed on 20 June 2018, serves to incorporate the GDPR legislative updates within the existing 1978 Law.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

Law No. 2018-493 grants new investigating and sanctioning powers to the CNIL. The major change of this law is that, except for the processing of certain sensitive data and data controllers no longer having to file CNIL declarations, data processing is no longer subject to former formalities. Through the GDPR, data controllers have more prerogatives, having to maintain a record of the processing of data and notify any data protection violation without undue delay.

The right to information and the right of access, rectification and deletion of personal data for the individual are reinforced and the sanctions in the event of obstruction or non-compliance with the legal provisions are increased. The CNIL has the power to impose a periodic penalty (limited to €100,000 per day) in addition to administrative fines (which can be as much as €20 million or 4 per cent of annual global turnover). CNIL agents also have a broader right to survey and investigate places used for the processing of personal data.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

The use of personal information must not impinge on an individual's right to privacy. Databases containing any kind of personal information must be established in accordance with European and French rules under the supervision of the CNIL. The GDPR will require careful consideration when conducting an internal investigation: without prejudice to any other grounds for cross-border transfers, that any transfer of personal data be based on international conventions.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

See question 29. Employees' communications through information technology devices made available to them by the company for professional purposes, are presumed to be professional and would therefore only be outside the scope of the company's right to intercept communications if they are identified as private. However, employees who benefit from a protective status because of their position in the company (social representatives, for instance) must be given working devices that prevent their communications being intercepted and their correspondents being identified.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Dawn raids are a key element of enforcement and evidence gathering in an overwhelming majority of cases by judicial and administrative authorities. However, external counsel should be contacted immediately, if for no other reason than to collect valuable intelligence about the investigation. There is little room for a company to object to a dawn raid if it abides by the rules framing the process and is authorised by the public prosecutor for *in flagrante delicto* and preliminary investigations or the investigating judge for judicial investigations. An important procedural rule is that, provided the raid does not relate to organised crime or terrorism, it may not start before 6am or after 9pm.

Companies should ensure they identify everything that is being seized, seek permission to make copies and specifically identify material that is attorney–client privileged or otherwise protected by law. If privileged materials are taken, they should be put under seal. Also, any incident should be reported in the minutes of the dawn raid and the minutes should not be signed if there is a disagreement as to content. Subsequently, if the legal requirements of a dawn raid have been violated, nullity of procedural steps can be obtained. The acts resulting from a raid, including the seizure of materials and all legal implications, will be considered ineffective. The company will therefore be able to apply for the return of the materials seized in the event that the raid did not comply with the legal requirements.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

There is a distinction to be made between external and in-house counsel. Legal privilege attaches to any advice provided by external counsel. Very often, privileged materials will be seized along with other material and a specific request must subsequently be filed to have the material covered by privilege returned to the company. There is no in-house counsel privilege, however, thus communications with in-house counsel are not protected by attorney–client privilege.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

An individual and (at least in theory) a company can refuse to answer questions based on the right against self-incrimination, and on the basis that the information is privileged. Provided there is no self-incrimination or information under privilege, an individual or a company that is not yet part of proceedings can be compelled to attend a hearing to testify – failure to do so incurs a €3,750 fine.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The first legal protection for whistleblowers dates back to 2007 and has developed since to target specific areas, including corruption and risks to public health or the environment. The Sapin II Law provides for a general whistleblower protection. Whistleblowers cannot be excluded from recruitment procedures or professional training, or face dismissal or discriminatory measures, whether direct or indirect, notably regarding remuneration. However, they are submitted to a three-tier process, consisting of a preliminary report to the whistleblower's supervisor and, in the event of that supervisor's failure to address the report within a reasonable amount of time, to the relevant administrative or judicial authorities or professional orders, and, as a last resort, to the public via the press.

In addition, France has two years to transpose a new whistleblower directive on the protection of persons reporting on breaches of European Union law dated 7 October 2019. This directive grants a broader protection to whistleblowers (beyond the scope of the work environment and applicable to their relatives). Unlike French law, the European provisions further provide for a two-stage process: disclose the information (1) internally, to the legal entity concerned, and (2) externally, to the competent national authorities, or to the relevant EU institutions, bodies, offices and agencies.

The idea of a financial incentive scheme was considered but the French Constitutional Council censored it. However, a Decree of 21 April 2017 set an experimental provision of two years that gave the General Directorate of Public Finance the authority to compensate any person, outside public administrations, who would provide information to lead to the discovery of tax evasion. This system has been perpetuated by the law of 23 October 2018 on

the fight against tax evasion. The directive, without providing a direct financial incentive, guarantees whistleblowers access to free and independent advice.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Data protection and privacy laws apply to all employees regardless of allegations of wrongdoing. Pursuant to French case law, messages sent by a company's employees using information technology devices made available to them by the company for professional purposes, are presumed to be professional. Hence, the employer is entitled to access the files and folders located on the company's computers or open messages within a professional messaging system without the employee being present, unless that employee has identified the material as personal. Nevertheless, the employee is entitled to invoke the right to privacy, which includes the secrecy of correspondence.

Officers and directors of companies who are subject to board decisions must be dealt with in the same way. In certain positions, which are subject to authorisation by a regulatory authority, removal of the authorisation can lead to termination.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

An employee deemed to have engaged in misconduct must be allowed the same rights as other employees (i.e., delay in being summoned for a prior interview and the application of legal and statutory conditions of sanctions).

If the misconduct is confirmed, an employer has a large set of tools to sanction the employee, including releasing the employee from his or her duties until completion of the investigation.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

An employee can be sanctioned for refusing to participate in an internal investigation, which is considered a sufficiently severe fault by the labour courts.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It should be considered good practice to prepare a document setting out the investigatory scope, especially when a judicial review seems likely by labour courts if an employee who is deemed to have engaged in misconduct challenges the findings of the internal investigations, for instance. The Paris Bar is due to publish detailed ethics recommendations for lawyers involved in internal investigations based on a report by Stéphane de Navacelle.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There is no obligation to report back to authorities nor is there a leniency programme. The company should assess the scope of the facts and the likelihood of a leak as soon as possible without creating unnecessary internal awareness.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

It is very likely that the enforcement authority would collect documents or data directly by conducting a raid within the company, having gathered sufficient information from third parties to ensure they are able to collect relevant information. If a company has any reason to believe a raid is likely, it should immediately ensure that any documents that may be seized are created in a privileged manner if possible, and consider providing separate representation to key employees. In some specific instances, it may make sense to reach out to the appropriate authority ahead of time.

Administrative authorities, for example the AFA, the AMF, the ACPR, the Competition Authority and the Ministry of Economy, can request communication of data and documents from companies under review or directly from third parties.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Other than obligations attached to publicly traded companies, there are no obligations as to when a company must disclose the existence of an internal investigation or contact from law enforcement. Self-disclosure is voluntary.

36 How are internal investigations viewed by local enforcement bodies in your country?

Having initially been embedded in legal culture, internal investigations have been accepted by specialised financial investigating magistrates as a necessary evil. Extra caution should nonetheless be taken if a judicial investigation is likely, as speaking to potential witnesses could be regarded as subornation and obstruction of justice, which is a crime in itself. It is useful to note that, in France, there is a monopoly on an investigation by the public authorities.

In a legal culture where negotiating a deal with a prosecutor or an investigating magistrate is uncommon, and as in-house counsel has no legal privilege, close attention will be paid to attorney–client privilege in internal investigations.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

There is no attorney–client privilege for communications with in-house counsel in France. For privilege to attach, the internal investigation should be carried out by external counsel, namely French lawyers admitted to the Bar. Interviewed employees are bound by contractual obligation to confidentiality, but this obligation cannot be used to avoid answering questions put by an investigating magistrate or police investigator. The Paris Bar released an opinion stating that professional secrecy applies between lawyers and their clients but does not apply to communications between lawyers and the employees of their clients when lawyers interview employees. Lawyers must therefore notify the employees of this, and their right to be represented by a separate attorney.

Professional secrecy applies to conversations between lawyers whether or not there is a common interest between their clients. Providing separate counsel to individuals is recommended to facilitate communications safely.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The principle of the attorney–client privilege was set down in Article 66-5 of the Law of 31 December 1971, amended by the Law of 7 April 1997 and by Article 226-13 of the French Criminal Code.

These provisions expressly set out that an attorney may not disclose information that contravenes professional secrecy. Article 226-13 of the French Criminal Code states that disclosure of secret information by persons entrusted with such a secret, by virtue of their position or profession, or a temporary function or mission, is sanctioned by imprisonment for one year and a €15,000 fine. Attorney–client privilege only applies when the lawyer is acting as a lawyer, that is to say, giving legal advice.

The holder of the privilege is the attorney's client, whether an individual or a company.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

No privilege attaches to communications with in-house counsel. Privilege only attaches to external counsel although the Gauvain Report dated 26 June 2019 recommends introducing a privilege applicable to legal advice given by in-house counsel.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Article 2 of the National Rules Procedure for Lawyers provides that the lawyer is of necessity the confidante of the client. Attorney–client privilege is a matter of public policy; it is general, absolute and unlimited in time. Subject to the strict requirements of their own defence before

any court and the cases of declaration or disclosure prescribed or authorised by law, lawyers may not make, in any matter, any disclosure in violation of attorney–client privilege.

There is no general provision regarding attorney–client privilege as regards foreign lawyers in relation to investigations. However, the Paris Bar Council has stressed that email exchanges between a client and a foreign lawyer are covered by attorney–client privilege. In addition, foreign lawyers can be temporarily and occasionally authorised to practise consulting and counselling activities in France. In that case, they are bound by both their home country's professional rules and the ethics rules applicable to French lawyers, which include attorney–client privilege.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Waiver of the attorney–client privilege is not specifically considered a co-operative step in France. The attorney–client privilege cannot be waived by the attorney under any circumstances, save for some exceptions (if an attorney must present his or her defence in a conflict opposing the attorney to his or her client). Only the client is entitled to waive the attorney–client privilege. At this point in time, there is still little reliance by enforcement authorities on internal investigations.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

This concept does not exist in France.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Privilege can be maintained in France after a limited disclosure abroad. However, co-operation between enforcement authorities would be likely to make the privilege moot.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privileges do not exist per se in French law. However, it is possible, for the purpose of defending a client, to share privileged information with other attorneys (without losing the privilege) – whether the clients share a common interest or not – and retained experts, such as forensic accountants.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

The scope of professional secrecy is very broad and lawyers are expected to rely on experts. That being said, it is usually safer to have the information collected and processed within the law firm's offices.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

There are no clear rules as regards internal investigations, and interviews with individuals who are not employees or former employees of the company should be considered with great caution. If the underlying facts amount to an offence under French law, such an interview would be likely to be considered an obstruction of justice. The proper alternative is to rely on external counsel.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

There are competing doctrinal opinions as to whether or not internal interviews are covered by attorney–client privilege. Attorney reports are covered by attorney–client privilege as long as the attorney is providing legal advice. On the other hand, attorneys' reports are not covered by attorney–client privilege if the attorney is providing an expertise assignment, as indicated in addendum XXIV to the Rules of Procedure of the Paris Bar published in 2016 by the Paris Bar Council. If this is the case, attorneys who draft an internal investigation report could be required to testify at a later stage in judicial proceedings.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Interviews of third parties should be ruled out unless specific precautionary steps are taken. The Paris Bar Council has issued recommendations, according to which attorneys should explain the purpose of an interview and its non-coercive nature to employees and inform them that their exchanges are not covered by professional secrecy (equivalent of *Upjohn* warnings). Employees should also be informed that they can be assisted by an attorney, but only when it appears that they may be blamed for their actions at the end of the investigation.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Assuming external counsel carries out the interview, they should explain both whom the attorney–client relationship is with and how the privilege rule works. Independent counsel should be provided to interviewees if there is any sense that they might be involved in any wrongdoing. Documents are usually provided ahead of time when counsel for the employee is involved, from the counsel for the company to the counsel for the employee directly, as correspondence between attorneys is covered by privilege. This ensures that the employee is not given the opportunity to communicate the documents to third parties and that the authorities are unable to seize such documents.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Except for specific crimes that are inchoate and can be avoided, only civil servants have a general obligation to report crimes of which they become aware in the context of their employment. There is no requirement to self-report. However, the guidelines on CJIPs clearly state that voluntary self-reporting of offences to prosecutors, if made in a timely manner, both as regards the choice of the CJIP procedure and as a factor reducing the amount of the public interest fine, will be taken into consideration favourably.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Except for antitrust issues, only in very limited circumstances does a corporation have an interest in reporting wrongdoing to enforcement authorities. It should first determine the scope of the wrongdoing and the responsibilities of those involved to assess potential corporate criminal liability. If the wrongdoing is carried out by a current or former employee, the corporation should weigh the pros and cons of filing a criminal complaint against the perpetrators to deter others, show commitment to compliance and shield itself from prosecution by acquiring the status of victim.

Self-reporting outside France should be based on a decision tailored to the foreign country's laws and enforcement policies. Should the company decide to self-report in a foreign jurisdiction, reporting the facts to French authorities should also be considered. Arguments to weigh up include the potential interest of French authorities in the underlying matter, where the facts occurred, whether they are continuing, and how closely national and foreign authorities work together. The SG CJIP suggests full co-operation between authorities and a real willingness on the part of the French authorities to take up investigations occurring in France or involving a French entity.

In more than 300 ongoing matters, the PNF is working closely on trying to address cases at the preliminary enquiry phase of criminal investigations before an investigating magistrate is appointed, namely, the instruction phase, which limits the leeway for plea bargaining and considerably extends the length of procedures.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

There is no specific procedure for self-reporting and no legal requirement to do so. Informal contacts should be made, through external counsel, with the competent authority, at the appropriate hierarchical level, after a thorough cost/benefit analysis. Although there is no statutory requirement to evaluate self-reporting and co-operation in a CJIP, the AFA and the PNF guidelines published on 26 June 2019 indicate that self-reporting within a reasonable period of time shall be favourably considered, in particular as a factor for reducing the fine.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

There is no common practice by enforcement authorities of providing advance notice to corporations that may become defendants in criminal procedures. Contact should be made with the police investigator, prosecutor or investigating magistrate depending on the status of the investigation. Challenges can be made against requests beyond the scope of the instruction from the judicial authority.

54 Are ongoing authority investigations subject to challenge before the courts?

Ongoing investigations led by the public prosecutor are not subject to challenge before the courts. Challenges are only possible once the investigation is closed.

Ongoing investigations led by the investigating magistrate can be challenged before the courts.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

The company should answer all the authorities involved separately, as the questions that can be raised by different authorities could vary, and it should be borne in mind that authorities communicate with one another. When dealing with foreign authorities, blocking statute, privacy and data protection issues should also be addressed.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

The collection of material abroad will have to be carried out in compliance with the applicable foreign law. However, national authorities will only be concerned about the actual answer to the production request.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

There is extensive co-operation with foreign enforcement authorities both within the European Union and elsewhere, through mutual legal assistance treaties, agreements between regulators and enforcement authorities, and EU co-operation agreements. With the SG CJIP having signed deferred prosecution agreements with the DOJ and the US Commodity Futures Trading Commission, this co-operation is even more visible.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Except where the law provides otherwise, and subject to a defendant's rights, enquiry and investigation proceedings are secret. Any person contributing to an investigation is bound by professional secrecy, and the disclosure of secret information is punishable by imprisonment for one year and a €15,000 fine. In practice, information is often leaked by people who are under no legal obligation and leaks to the press in sensitive matters occur very frequently.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The company should retain external counsel to explain the foreign country's law to the requesting French authority, and work with the French and foreign authorities for the production to be carried out appropriately, possibly pursuant to formal co-operation agreements.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

France has both blocking and data protection and privacy statutes. The French blocking statute, subject to treaties or international agreements and to currently applicable laws and regulations, prohibits communication to foreign public officials of economic, commercial, industrial, financial or technical information or documents if that communication is harmful to France or is to be used as evidence in view of foreign judicial or administrative proceedings or in relation thereto. Secrecy should also be properly addressed when a notice or subpoena concerns a bank: banks owe a legal duty to their customers not to disclose information about their affairs to third parties. Breach of this duty is criminally sanctioned pursuant to the French Monetary and Financial Code and the French Criminal Code. To ensure that the blocking statute, the data protection law and, if applicable, banking secrecy, do not affect domestic enforcement, the communication should be properly addressed when responding to a foreign authority.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Voluntary production is limited to very specific circumstances, mostly when foreign authorities are involved, or when, in an ongoing investigation, there is a strategic interest to do so. Criminal files are accessible to all parties involved, including victims and other defendants. Although legally covered by secrecy rules for legal professionals, parties themselves are free to share information from the file – not documents – with third parties. Information from high-profile cases is regularly leaked to the press.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Corporate liability does not shield individuals from liability. In an overwhelming majority of cases (as required by law), the courts have to identify the individual or organ acting on behalf of the company (see question 2).

Penalties for individuals include fines, imprisonment, payment of civil compensation to victims within the same criminal procedure and prohibition from specific managerial positions in addition to publication of the decision in the press. Except for imprisonment, penalties for companies include all the above, as well as dissolution and debarment for certain specific offences.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Ordinance No. 2015-899 of 23 July 2015, which transposes Directive 2014/24/EU on public procurement, prohibits companies found guilty of specific offences (e.g., corruption, fraud, money laundering, terrorism or embezzlement and misappropriation of property) from competing for government contracts throughout the European Union. This exclusion is automatically for a period of five years unless the sentencing decision specifically provides for a more limited period (Article 45 of the Ordinance). Article 39 of the Sapin II Law amended Article 45 of the Ordinance, which now allows a declaration on honour as sufficient proof that the candidate is not prohibited from applying for a government contract.

64 What do the authorities in your country take into account when fixing penalties?

Although laws provide for very high penalties, including those based on a percentage of overall revenues for companies, penalties will be based on net worth, income, personality and *mens rea*. Although not recognised as such by law, deterrence appears to be a growing component of the rationale for penalties.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Non-prosecution agreements are not part of the French legal system. Deferred prosecution agreements (DPAs) are slowly becoming part of the legal system. The Sapin II law provides for a DPA procedure limited to corruption and 'probity offences': the CJIP. Plea agreements – also limited to specific offences – have been available for more than a decade.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

There is no such reporting restriction under French law outside applicable labour law that the individual could invoke against the company at a later stage. Far from providing reporting restrictions, the recently published CJIP guidelines provide that the aim of internal investigations conducted by a prosecuted company is also to determine individual liabilities. To that extent, keys witnesses shall be identified and, if interviews have been conducted with witnesses or with persons likely to be involved, the reports shall be communicated to the prosecutor.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

There is an increasing recourse to the pretrial guilty plea procedure (CRPC) and CJIPs in France. The Sapin II law provides for CJIPs limited to instances of corruption and 'probity offences'. Companies should move swiftly to settle if possible, as both procedures provide for, and are likely to include, forceful involvement of alleged victims who will pursue their own interests. If the case may involve foreign jurisdictions, companies should assess the consequences of admitting guilt in France.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

The AFA was empowered by the Sapin II Law to supervise companies as part of the implementation of CJIPs. Among the obligations imposed by the CJIP is the implementation of an action plan, as required, with the aim of improving the company's compliance system under the AFA's control for a maximum of three years. In such cases, the AFA can be helped by law firms and experts. During the past two years, of the six companies that entered into a CJIP, four designated the AFA as a compliance monitor.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Parallel private actions are possible. In most instances, alleged victims will join the criminal procedure as civil parties and, as such, will be granted full access to the files and be able to submit requests for investigative steps to investigating magistrates. Also, alleged victims can start a criminal investigation by filing a specific complaint to that effect.

Private parties do not normally have access to administrative authorities' investigation files.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Secrecy at the investigatory stage is required by law. However, defendants and victims have access to the file. It is sometimes very difficult to keep communications and information taken from the criminal file private. Once a case is before a court, the press can cover the event, be present at the hearing (albeit microphones and cameras are prohibited) and attend the debates. Defendants and victims are free to make statements.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is very common to have press releases, communications and crisis management strategies prepared, and, when appropriate, public relations firms assisting. The spokesperson is often a lawyer on the case, especially when individuals are involved.

72 How is publicity managed when there are ongoing related proceedings?

Publicity is part of the overall strategy, especially in high-profile matters that attract political attention and have numerous civil parties.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Unless otherwise specifically requested by an agreement, there is no obligation to disclose settlements to the public. In anti-corruption matters, the Sapin II Law makes disclosure compulsory. Any settlement in criminal matters will have to be approved by a judge at a public hearing. Although investigative measures and the results of investigations are to remain confidential, and police officers, judges and legal experts are bound by that confidentiality, administrative authorities are permitted to communicate on sanctions and settlements.

It is interesting to note that CJIPs do not amount to an admission of guilt in France and companies will not have a criminal record, thus allowing them to still participate in public procurement proceedings.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

France is quite proactive. The Gauvain report entitled 'Restoring French and European sovereignty and protecting our companies from extraterritorial laws and measures' (published on 26 June 2019) recommends a number of legal changes with the aim of strengthening the French legal framework applicable relating to foreign procedures initiated against French

companies. The main recommendations include strengthening the blocking statute by heightening applicable sanctions and by making sure that requests for information go through the competent channel (the Economic Strategic Information and Security Department); introducing a legal privilege applicable to in-house counsels; and protecting French companies' data against the Clarifying Lawful Overseas Use of Data Act (or US Cloud Act, enacted in 2018) by imposing administrative fines similar to those applicable for violations of the GDPR (up to 4 per cent of annual global turnover or €20 million) in the event of transmission of any such data by US data hosting companies outside applicable international agreements or treaties.

14

Germany

Eike Bicker, Christian Steinle, Christoph Skoupil and Marcus Reischl[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The diesel emissions cases involving several German carmakers continue to be the highest-profile corporate investigations in Germany. The automotive industry is one of the key German industries and the emission investigations against several major German car manufacturers have therefore attracted a lot of public attention. Furthermore, the high volume of damage allegedly suffered by customers, investors and others, and the technical and regulatory complexity of the topic, are remarkable. The criminal investigations by various German public prosecutor offices focus on individual criminal liability of managers, including former chief executive officers, while at the same time leading to triple-digit millions of euros in fines against the companies involved.

2 Outline the legal framework for corporate liability in your country.

Even though strict corporate criminal liability is under discussion *de lege ferenda* and may be introduced within the next year, under current German law, companies are technically not criminally liable. Instead, companies whose employees have committed criminal or administrative offences face the risk of an administrative fine or a confiscation order.

These administrative fines are capped at €10 million, though this amount can be – and, in practice, frequently is – exceeded by the financial benefit the company has obtained from committing the offence (i.e., profit disgorgement). This legal mechanism (administrative fines plus profit disgorgement) have led to quite significant fines in the past, as in

1 Eike Bicker and Christian Steinle are partners and Christoph Skoupil and Marcus Reischl are associated partners at Gleiss Lutz.

the following cases: *Siemens* (€395 million), *MAN* (€150 million), *Ferrostaal* (€140 million), *Volkswagen* (€1 billion) and *Audi* (€800 million).

As an alternative to an administrative fine, a confiscation order can be imposed on a company if an unlawful act has been committed. The maximum amount for a confiscation order is the entire gross value of the proceeds from the respective criminal offence, and the fined party (i.e., the company) is not permitted to deduct any costs it incurs.

Recently a draft bill concerning corporate criminal liability (Draft Corporate Sanctioning Act) became public. The new law will change the landscape for compliance and investigations in Germany significantly. Penalties are being increased to up to 10 per cent of the group's global turnover, although they may be reduced if the company has initiated an independent and state-of-the-art internal investigation, and co-operates fully with the investigating authorities. The Draft Corporate Sanctioning Act further introduces an alternative for ending proceedings, similar to a deferred prosecution agreement or non-prosecution agreement, including the possibility for the court to order the appointment of a compliance monitor.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Various law enforcement authorities, at both federal and state levels, regulate corporations, including, among others, the public prosecutors offices, antitrust authorities, tax authorities, financial regulators and customs authorities.

The matter of jurisdiction between the authorities depends on the scope of the potential investigation. To this extent, various areas of responsibility are assigned to specialist authorities. It is important to understand that all 16 German states have their own prosecutors, and thus some of them are more active in prosecuting corporations (e.g., Munich, Frankfurt and Stuttgart) than others.

There are no guidelines for the investigation of corporations in the form of laws or legal regulations. However, we are aware of some internal guidelines drafted to assist authorities when investigating corporations.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The public prosecutor's office is generally obliged to take action in relation to all prosecutable criminal offences, provided there are sufficient factual indications (or initial suspicion). However, this duty of legality pertains only to criminal offences. Therefore, the public prosecutor has discretion whether to open administrative proceedings against a corporation (see also the mechanisms of corporate fines described in question 2).

This would change with the Draft Corporate Sanctioning Act and the mandatory prosecution principle would also apply to the prosecution of companies.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Enforcement measures taken by authorities against suspects or witnesses (e.g., search warrant, confiscation) can be subject to, inter alia, judicial review. This applies to the order itself as well as to the manner of execution.

Subpoenas as such are not challengeable. However, potential enforcement measures or court decisions following a subpoena may be challenged. In German criminal proceedings, the defendant is not obliged to co-operate with the authorities or to provide information about evidence-relevant facts.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Generally, the public prosecutor cannot grant immunity or leniency to individuals who assist or co-operate with investigations. However, prosecutors and courts regard co-operation as a major factor in determining the level of sentences. Furthermore, in certain cases, prosecutors have some discretionary powers to dispense with the prosecution with the consent of the accused and of the court, and co-operation is certainly a factor in this decision.

The German antitrust authorities can grant cartel participants who co-operate, and thereby contribute to uncovering a cartel, immunity from or a reduction of fines. This leniency programme is available to individuals as well as companies. Full immunity will be granted to cartel participants if they are the first to disclose the cartel and fully co-operate with the antitrust authority throughout the proceedings.

7 What are the top priorities for your country's law enforcement authorities?

Corporations in Germany are most severely prosecuted for antitrust violations and corruption. The highest fines are regularly imposed in both these areas. In the recent past, fraud and tax fraud proceedings have also been a priority (for instance, alleged irregularities regarding diesel engine emissions and cum/ex or cum/cum trading patterns of banks and financial institutions). We expect data protection violations and the betrayal of business and company secrets to attract more enforcement activity as a result of stricter legal regulations and increased sanctions.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Since 2015, the issue of cybersecurity has been addressed by various laws and regulations in both German and European legislation, including the German IT Security Act, the EU Directive on Network and Information Security and the EU Cybersecurity Act. This legislation addresses the cybersecurity landscape without imposing any specific duties on individuals or companies.

Under the EU General Data Protection Regulation (GDPR), companies that are processing personal data must implement appropriate technical and organisational measures

to ensure a level of security that is appropriate to the risk. A violation of this duty can trigger administrative fines and claims for damages. As regards data breaches, companies may be obliged to notify supervisory authorities and the individual data subjects.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Cybercrime, that is criminal activities carried out by means of computers or the internet, is covered by general German criminal law pursuant to a variety of specific provisions regarding data espionage, computer fraud, data forgery, deception in the context of data processing and data tampering.

Cybercrime investigations are seldom only national in scope. They call for coordinated action at international level and require a high level of cross-border co-operation. As an EU Member State, Germany is a signatory to the Convention on Cybercrime, which includes provisions on international co-operation with the other EU members and further signatories, such as the United States, Japan and Australia.

On the practical side, law enforcement authorities have implemented cross-border communication networks and coordination units, including the Interpol Global Complex for Innovation, the European Cybercrime Centre at Europol, and others.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

German criminal law is generally applicable if either the offender acted in Germany or the offence had a consequence in Germany. Furthermore, Germany implemented the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of the Organisation for Economic Co-operation and Development in 1999. Since then, the German Criminal Code prohibits illicit payments to foreign public officials, in a similar way to the US Foreign Corrupt Practices Act and the UK Bribery Act. In addition, bribery payments in the private sector that exclusively affect foreign competition, are covered by German law.

Furthermore, German criminal law is applicable, among other reasons, if the offence is committed abroad against a German or if a German commits an offence abroad and the act is a criminal offence at the place where it was committed as well.

Under the Draft Corporate Sanctioning Act, a corporation could be sanctioned for corporate crimes abroad if the corporation is registered in Germany.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border investigations generally demand a high level of sensitivity with regard to the different expectations of the authorities involved and the different legal frameworks applicable to investigative steps in different countries.

If an investigation has links to a common law jurisdiction, privilege is often a topic because the principles of legal privilege differ. As the concept of pretrial discovery does not exist under German law, privilege is only relevant in relation to law enforcement authorities. Under German law, communication between a company and its legal advisers is not generally privileged, but the concept of legal privilege is limited – in most cases – to communication with the criminal defence counsel. The disclosure of separate information to public authorities does not generally put the legal privilege at risk.

To ensure that privilege is adequately protected, cross-border investigations require clear processes in line with the privilege provisions of all the jurisdictions involved.

Differences in data protection laws are relevant in cross-border investigations outside the European Union where the GDPR is not applicable. In cross-border investigations, information is gathered in and transferred from and to different jurisdictions, and breaches of applicable data protection laws must be avoided.

When interviewing employees, employment law has to be observed. In Germany, broadly scoped investigative measures may require the involvement of the works council.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Companies are not protected, in principle, from sanctions in Germany after having resolved charges on the same core set of facts in another country outside the European Union (see, for example, the fines imposed against Volkswagen in the emission matter in the United States and Germany, or the fines imposed by German and other antitrust authorities in cross-border cartel cases based on the local effect in their respective jurisdictions). In addition, confiscation orders and similar measures against companies are not recognised as 'sanctions' in the sense of double jeopardy, so that companies are not yet effectively protected in this regard even within the European Union. Often, however, authorities consider a (potential) foreign sanction at their discretion when determining a (national) sanction.

To avoid double jeopardy, the Draft Corporate Sanctioning Act provides for the possibility to refrain from national prosecution if sanctions by foreign authorities are expected and the potential sanctions in Germany do not carry substantial weight or are not necessary from a preventive point of view.

13 Are 'global' settlements common in your country? What are the practical considerations?

There is no legal framework for 'global' settlements under German law. However, as co-operation between authorities across borders generally increases, 'global' settlements with German authorities are generally achievable, at least to some extent. In the past, German authorities sometimes took account of foreign sanctions when determining a (national) fine (e.g., the *Siemens* case).

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

In principle, the decisions of foreign authorities have no (legal) effect on an investigation of the same matter in Germany (see question 5). In some cases, however, German and foreign authorities coordinate with each other to avoid duplicate investigations.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Authorities are making increased use of the sanction options described in question 2. In 2018 and 2019, fines of €1 billion, €800 million and €535 million were imposed on Volkswagen, Audi and Porsche, respectively, in connection with potential irregularities regarding diesel emissions. Further, significant fines were imposed in antitrust proceedings and cases of corruption (*Siemens*, €395 million; *MAN*, €150 million; *Ferrostaal* €140 million).

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Sanctions enforcement activities have steadily increased in recent years, although there are still considerable differences across the 16 German states. We expect a further increase in the intensity of prosecution if corporate criminal liability legislation is passed, whereby the mandatory prosecution principle would be extended to the prosecution of corporate offences.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

In some cases, there is co-operation between national and foreign authorities. This possibility has been codified in the form of mutual legal assistance, within the framework of which formal enquiries can be made.

In our experience, there is also an informal exchange between national and foreign authorities. However, there is often no such co-operation because of the effort involved and the sometimes low yield.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

According to German law, a boycott declaration is prohibited (this does not apply to resolutions of the United Nations, the European Union or Germany).

In addition, the EU Blocking Regulation applies in Germany. The Regulation prohibits all companies registered in the European Union from complying with the US acts listed in the Annex to the Regulation (which are currently mainly US sanctions against Iran), unless exceptionally authorised to do so by the European Commission. Furthermore, the Regulation enables such companies to seek compensation if they suffer damage as a result of

those US acts. In addition, judgments by foreign courts (in particular those of the United States) that are imposed to enforce the sanctions are not recognised in the European Union.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

A violation of the national and European blocking legislation is punishable by fines of up to €500,000. Furthermore, there is the risk that legal transactions in violation of the EU Blocking Regulation may be null and void or that violations of that Regulation may trigger contractual claims for damages by the affected business partner.

So far, the Regulation has not been applied in practice. There is therefore no known case in which administrative offence proceedings have been initiated for an infringement.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct come to light in many ways. In practice, investigations into serious wrongdoing are most often initiated by whistleblowers or as a side effect of running internal investigations.

Information gathering

21 Does your country have a data protection regime?

Yes. Data protection law in Germany is regulated by the GDPR and the national German Data Protection Act. Further, there are various provisions on data protection law in sector-specific legislation (e.g., the German Telecommunications Act).

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

With the introduction of the GDPR, the situation for companies in the European Union has changed substantially. Previous to that, only a limited number of fines were imposed for data protection breaches. Now, companies can face a maximum fine of €20 million or 4 per cent of their annual global turnover, whichever is higher. Although authorities have so far not exhausted this penalty range, the level of company fines has increased significantly since the introduction of the GDPR in May 2018.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

The collection and use of personal data from employees during internal investigations has to be in line with the GDPR and the German Federal Data Protection Act, and this applies in particular to email and data reviews as well as interviews. For each investigative step involving the processing of personal data, one must assess whether the processing is necessary for the purposes of the legitimate interests pursued by the company and whether those interests of

the company are overridden by the interests or rights of the respective data subject. Specific requirements apply with regard to employees when the private use of company information technology is allowed. Furthermore, affected employees have to be informed about the subject and purpose of the investigation, and their rights under the applicable data protection laws, unless doing so would interfere with the integrity of the internal investigation. The involvement of entities other than the employing entity typically requires the conclusion of data protection agreements. Works council agreements (concluded to comply with German labour law) can stipulate further requirements.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

The live monitoring of employees' communications is not explicitly prohibited under German data protection, criminal and labour laws, but the threshold for justifying measures of this kind is high and requires, inter alia, a thorough weighing of the company's interests – including the possibility of less invasive measures – against the rights and interests of the respective employee.

The review of historic email and other communication data is generally permitted if justified by legitimate interests of the company and if there are no overriding interests of the respective employee. To preserve proportionality, some specific rules for data reviews have to be observed, such as the exclusion of private data, search term filters and independent reviewers obliged to secrecy. The employee's prior consent would only justify the processing of the data if it is given freely on an informed basis, which can generally be disputed in hierarchical structures.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

In the course of criminal or cartel proceedings, companies are often subjected to search and seize measures. The relevant orders must, inter alia, include the facts giving rise to the suspicion and be proportionate.

Affected companies can, among other remedies, apply for a judicial review of such a measure or defend themselves against it by means of a judicial complaint. In practice, however, such legal remedies are mostly unsuccessful.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

The conditions under which documents from internal investigations in Germany are exempt from seizure are largely unclear. To protect (potentially) privileged documents, the following measures, among others, may be taken:

- enter into an attorney–client relationship with the company affected by an investigation (and not, for example, its holding company) and document that the purpose of the mandate is (at least) to defend the company;

- do not establish client's possession of work products at risk of seizure;
- take organisational measures to separate documents that are expected to be seizable from documents that are expected to be privileged; and
- label correspondence and documents as 'privileged' or similar.

The Draft Corporate Sanctioning Act could have a significant effect on the protection of attorney work-product. According to the official explanation to the draft bill, documents from internal investigations shall be seizable, even if they are held in the custody of lawyers, unless the client is formally a defendant in criminal proceedings and there is a 'relationship of trust' with regard to the documents. Practitioners in Germany have – rightly – criticised this interpretation and it is possible that it will be changed in the course of the further legislative proceedings.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Defendants have the right to remain silent towards the authorities and do not need to actively participate in the investigation (i.e., the right not to incriminate oneself).

Witnesses (at least in public prosecutors' offices and courts) are obliged, in principle, to provide information. As an exception, they may refuse to testify if (1) they are related to the defendant or (2) their testimony would expose them or a relative to the risk of prosecution.

If the witness is subject to the obligation of professional secrecy (as are lawyers), testifying may be refused in this regard.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

There is currently no general legal framework for whistleblowing in Germany. In April 2019, the European Parliament passed the EU Whistleblowing Directive, and the European Council is expected to confirm it in the near future. The EU Member States will then have two years to implement laws aimed at strengthening whistleblower protection in line with the Directive. From then on, at least larger companies will have a duty to implement whistleblowing systems. Whistleblowers who act in good faith will be protected from any retaliation if they report misconduct to the company or the competent authority.

Until this legislation has been passed, German law provides protection for whistleblowers under general labour law principles and some specific provisions, such as with respect to the reporting of safety-at-work issues and prohibited uncovered short sales.

Currently, there is no general duty on German companies to implement whistleblowing structures under German law except for financial institutions (section 25a of the German Banking Act).

Financial incentive schemes for whistleblowers are not common in Germany and are not expected to be implemented in the near future. However, as already discussed (see question 6),

if the whistleblower is one of the perpetrators, disclosure to the authorities may well reduce a potential sentence significantly (see section 46b, German Criminal Code). In cartel cases, the fine to be imposed on a cartel participant is even waived if he or she is the first to contact the German cartel authorities to uncover the cartel.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employees are generally obliged to co-operate with internal investigations and no distinction is made here between employees who are suspected of having committed a wrongdoing and those who have potential knowledge about a wrongdoing or just the circumstance surrounding it. Employees are obliged to co-operate even if their co-operation could result in them being convicted for specific crimes.

If an employee co-operates with an internal investigation, the company may have to cover the costs of the employee's legal counsel, subject to a case-by-case analysis.

German data protection laws impose specific information duties on employers that process employees' information in the course of an internal investigation. Affected employees have to be informed about the subject and purpose of the investigation and their rights under the applicable data protection laws unless doing so would interfere with the integrity of the internal investigation.

The duty to co-operate applies in the same way whether the individual is an employee, an officer or a director. However, directors are not just obliged to co-operate with internal investigations but may be obliged to actively initiate and conduct them.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Although there is no general differentiation between employees under suspicion and others, German labour and data protection laws require the weighing of the employee's interests against those of the company's before measures are taken that affect the employee's rights. The degree of suspicion against an employee may tip the scales in this context.

Under German corporate law, a company's management board must investigate potential misconduct and must put a stop to any misconduct discovered, revise the compliance programme and the internal controls affected and take steps, including relating to personnel, as a result of the misconduct. Therefore, the management board may be required to transfer or even give certain employees their notice, based on a thorough case-by-case analysis.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

In general, employees are obliged to co-operate with internal investigations, even if this could incriminate themselves. Depending on the specific case and the impact of the refusal, an employee may be dismissed if he or she refuses to co-operate.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Yes, an investigation plan is key to an efficient and successful investigation. An investigation plan would normally include the scope of the investigation, the respective responsibility of the company and the law firm, the steps to be taken, the data and documents to be collected and the custodians.

The investigation plan is an important starting point and requires ongoing revision subject to the findings made and the obstacles encountered.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

The concrete steps to be taken in this situation really depend on the nature of the issue discovered. Generally, German corporate law imposes certain duties on the company's management board if there are indications of misconduct. First, the management board has to investigate the potential misconduct and put a stop to it. Second, the management board has to revise the compliance programme and the internal controls affected and take action, potentially including relating to personnel, as a result of the misconduct.

To a certain extent, the management board can delegate those obligations to internal department (e.g., compliance). However, to fulfil the board's supervisory duty, regular reporting to the management board of incidents handled by the internal departments is required. If an issue comes to light that points to severe misconduct or a matter that is potentially of high risk for the company, the management board should be notified immediately.

Although there is no general duty to report misconduct to the competent authority, reporting may be required in some specific cases. In particular, misconduct with a tax implication for the company has to be reported to the tax authorities in the vast majority of cases.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

First, it is generally advisable to enforce a litigation hold and to collect the respective data. This step should further be extended to documents and data in the relevant context and should not be restricted to the documents and data requested by the law enforcement authority.

In a second step, the company will have to assess whether it is actually obliged to produce the requested data and documents. Independently of the result of this assessment, the company will have to answer the question whether it is willing to co-operate and will have to find a strategic position regarding the authority. In many cases, it is advisable to co-operate with the authority to prevent coercive measures and reputational damage.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

In general, there is no duty to publicly disclose the existence of an internal investigation or contact from a law enforcement authority. Whether a disclosure is made or not largely depends on the interests of the company in the specific case.

Exceptionally, stock listed companies may be subject to a disclosure requirement if the investigation has an effect on the company that would be likely to have a significant effect on the company's stock price (ad hoc announcements).

36 How are internal investigations viewed by local enforcement bodies in your country?

Especially in larger and complex proceedings, authorities welcome internal investigations as part of a company's pledge to co-operate with a criminal investigation. In our experience, in most cases, authorities take into account the costs of an internal investigation when it comes to sanctions and fines if the internal investigation is done properly and the company has co-operated fully with the authority.

As far as possible, the measures to be taken as part of an internal investigation conducted in parallel with an official investigation should be coordinated with the authorities. Otherwise, there is a risk that an authority might feel obstructed by an internal investigation and that a possible bonus could turn into a handicap.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

German case law is inconsistent on this issue. In principle, protection against seizure depends on whether (1) the company is already under an official investigation or at least objectively likely to be officially investigated and (2) the relevant documents are drafted for defence purposes.

To protect potentially privileged materials, the protective measures described in question 26 may be taken.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The key principles are as described in question 37. In general, these principles are true for both companies and individuals.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The exemption from seizure as outlined in question 37 applies in principle only to defence communication with external counsel.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Protection from seizure can also cover work-product of foreign lawyers drafted in their capacity as defence counsel. International attorneys, however, may be subject to restrictions as to their ability to appear in court.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

The disclosure of privileged documents is generally regarded as a co-operative step by national authorities. However, there is no general concept of waiving privilege under German law.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

There is no concept of limited waiver of privilege in Germany.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Waiving privilege in another country has no direct legal effect on privilege claims in Germany. However, it is possible that the waived documents may be seized from the third person abroad if he or she does not enjoy protection against seizure under German law.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privilege does not exist in Germany.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

The question as to the extent to which assistance should also be included in protection against seizure has not yet been conclusively clarified by case law. As a rule, the further documents leave the sphere of an external counsel, the weaker their protection.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Interviews are an important and common part of internal investigations in Germany.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

National case law is inconsistent on this issue. In principle, protection against seizure depends on whether (1) the company is already under an official investigation or at least

objectively likely to be officially investigated, and (2) the relevant documents are drafted for defence purposes.

In the case of interview protocols and attorney reports, it should be argued that these work-products also serve as preparation for corporate defence and are therefore privileged.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

An employee is generally obliged to co-operate with internal investigations and to tell the truth even at the risk of self-incrimination. This may not apply to interviews of third parties, such as former employees.

As many employees are not aware of their duty to tell the truth, it is customary to inform them about it in an introduction. Other customary elements of the introduction, if applicable, are:

- information that the legal counsels conducting the interview are lawyers of the company and are not acting for the interviewee;
- the possibility of an employee engaging his or her own attorney and clarification about the costs (if relevant and to prevent disruption, this information may already be provided in the invitation to the interview);
- the company may choose to share parts or all information provided in the interview with national or foreign courts, or law enforcement authorities;
- refusing to co-operate may lead to disciplinary action;
- the modus of the protocol, whether the employee will be granted access to it and whether he or she will have to confirm its content; and
- the employee's data protection rights, ideally accompanied by such information in writing.

Essentially, this information is very similar to the *Upjohn* warning concept developed in the United States.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

A state-of-the-art interview in Germany usually begins with a briefing about, inter alia, the subject of the interview and the interviewee's rights as set out under question 48. The interview environment should be appropriate (e.g., a neutral meeting room on the company's premises or at the law firm's offices) and – depending on the duration of the interview – sufficient breaks, drinks and food should be offered.

Depending on the stage of the internal investigation, documents may well be shown to witnesses during interviews.

German case law is not yet settled on the question of whether an employee has the right to be accompanied at an interview by his or her own counsel and who has to bear the costs. However, companies usually allow interviewees to have a legal representative of their own in attendance, at least in cases where the company is represented as well. In the recent past, there have been discussions as to whether an employee's right against self-incrimination in

internal investigations shall be introduced into German law. According to the new Draft Sanctioning Act, employees may (indirectly) be granted the right to remain silent if they risk self-incrimination.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

In principle, there is no obligation in Germany to report misconduct to law enforcement authorities. Exceptionally, however, individual statutory regulations may require a report. This applies, inter alia, in connection with incorrect tax returns and in the field of money laundering.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

This depends on a comprehensive analysis in each particular case. Generally, in cases where there is a high risk that the competent authorities may get hold of the information, or the company's future business may be compromised as a consequence of the undisclosed misconduct (e.g., if a declaration of honour cannot be signed), disclosure may be advisable.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

First, you should make sure you have the right timing, in particular with respect to the ongoing investigations. Then, the company representative should contact the competent authority and set a meeting for initial discussions based on a summarised set of facts, including evidence. During this meeting, the further proceedings should be agreed mutually.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

This will depend on the status of the investigation and the negotiations. It is generally possible to discuss requests made by the authorities. It is important to understand that, although there is no legal duty to reply to requests for information in criminal investigations, refusal to do so is likely to lead to a raid by the law enforcement authority.

54 Are ongoing authority investigations subject to challenge before the courts?

The investigation itself cannot be challenged in court.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Preventing inconsistent communication with different authorities is certainly important. However, it should be considered that, in particular in complex investigations, different authorities develop different focus areas, for example as a result of a different legal assessment.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In principle, companies are legally not obliged to produce any material from abroad. However, refusal to do so could lead to legal assistance requests from German authorities to their foreign counterparts and would be seen as unco-operative, thus jeopardising any co-operation bonus. Therefore, it might be advisable to produce the documents outside Germany, provided the company has the power to do so under company law. In situations such as this, the company is also obliged to respect local laws, in particular data protection laws.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

As already discussed in question 9, law enforcement authorities have implemented cross-border communication networks and coordination units to co-operate effectively, and we have see a rise in international co-operation. The legal framework is fragmented and includes EU regulations as well as bilateral and multilateral treaties.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Generally, investigating officers are bound by confidentiality with respect to information received in the course of an investigation. However, third parties may have a right to access the investigation file or parts of it, for instance to prepare civil claims against the perpetrator.

Public officials in the tax authorities are additionally obliged to observe tax secrecy (under section 30, German Fiscal Code).

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Subject to a thorough assessment of the local law prohibiting the production, we would generally advise complying with applicable law and trying to convince the German authority either to forego the requested documents or to seek administrative co-operation to formally seize the documents locally.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

See questions 18, 19 and 59. We would generally advise engaging with the investigating authorities to evaluate alternatives.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Before voluntarily producing documents, privilege issues in cross-border situation have to be considered. In addition, in the case of voluntary production, increased attention should be paid to data protection aspects. With respect to confidentiality, there are no relevant distinctions between voluntary production and compelled production under German law.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Individuals can, in particular, be sanctioned by fines or imprisonment. They may also be banned from carrying on their profession.

For companies, fines and profit confiscation are particularly relevant. In addition, exclusion from (public) tenders can have a significant negative effect on companies (see questions 2 and 65 regarding potential changes that may be introduced with the Draft Corporate Sanctioning Act).

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

A debarment under German public procurement law can also be based on misconduct of the company or its employees abroad. To mitigate this risk, a settlement abroad should be accompanied by self-cleansing and remediation measures by the company in Germany. These may include, inter alia, disciplinary measures against the individuals involved, compensation for damage sustained, co-operation with investigating authorities, and strengthening of the compliance management system.

64 What do the authorities in your country take into account when fixing penalties?

Authorities take into account, inter alia, the degree and extent of the misconduct committed, the subjective accusability of the misconduct, economic circumstances and the extent to which the parties concerned have co-operated with the investigating authorities. In addition, the Federal Supreme Court recently decided that the design of a compliance management system and the extent to which it was adapted at the time of the misconduct, and the improvements implemented after the misconduct, must also be taken into account.

The Draft Corporate Sanctioning Act, in particular, and in addition to the criteria set out above, allows for a reduction in sanctions imposed on corporations if the company initiates an internal investigation and fully co-operates with the authorities. To be eligible for such a reduction, the internal investigation must (1) be independent (i.e., not conducted by the company's defence counsel), (2) be fair and (3) make a material contribution to clarifying the corporate misconduct. Further, the company must co-operate continuously and unrestrictedly with the prosecuting authorities, and the results of the internal investigations, the essential documents and the final report on the internal investigations must be disclosed to the prosecuting authorities.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Not at the moment. Currently, settlements with authorities are reached via a 'negotiated' fine or confiscation order where the misconduct and the facts are described. Under German law, neither the order nor the statement of facts are public. Nevertheless, in high-profile cases, the authorities usually issue a short press release summarising the facts and the case (approximately one to two pages). The settlement need not be approved by the court, but lies in the discretion of the public prosecutor. German authorities often expect the company under investigation to improve their internal structures before a settlement is made in order to achieve a decent deal.

The current German federal government seeks to revise the corporate sanctions regime.

The Draft Corporate Sanctioning Act offers the alternative of ending proceedings by warning the undertaking, reserving the right to impose penalties and, in some cases, tied to conditions and directives during the period for which such a right is reserved. In such cases, the court may additionally order the appointment of a compliance monitor.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

No.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Companies should consider in particular the economic and reputational effects of the settlement itself, the (regularly positive) consequences of terminated investigations for the operational capacities of the company, the consequences for public procurements (e.g., potential debarments in Germany or abroad), further co-operation with investigations against individuals and the structural consequences to be drawn to prevent similar misconduct in the future.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

See question 65. At the moment, corporate compliance monitors are not foreseen by the law and are therefore not used in Germany. However, the Draft Corporate Sanctioning Act, if enacted, would introduce compliance monitors as a procedural instrument to enable deferred prosecution.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Parallel private actions are allowed. In some cases, however, civil courts tend to suspend proceedings until criminal proceedings on the same subject have been completed.

Private plaintiffs may have the right to access criminal files if, inter alia, they present a legitimate interest in this, and if this is not opposed by the overriding interests of the defendant or other persons who are worthy of protection.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

In principle, investigations are not public. However, they regularly become publicly known if the case is interesting enough. Apart from a few exceptions, criminal trials are public.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

This depends on the specifics of the case and the in-house capabilities of the company. In larger cases where public opinion is of an elevated relevance, the engagement of public relations consultants is quite common. The communication strategy needs to be fully aligned with the company's internal findings and legal defence strategy. In our experience, the communication strategy should strike a balance between 'litigation language' and frank and honest communication.

72 How is publicity managed when there are ongoing related proceedings?

Usually, no substantial public statements on the allegations should be made while the facts are still under investigation. If possible, next steps can be communicated.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

This must be assessed on in each particular case, taking into account all rights and legitimate interests of the company, its shareholders and the authorities involved.

Anticipated developments

74 **Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?**

Following a programmatic agreement of the grand coalition, Germany's Federal Ministry of Justice has unveiled the draft of a new Corporate Sanctioning Act, introducing corporate criminal liability in Germany and significantly ratcheting up corporate liability for business-related criminal offences. The draft bill:

- raises possible penalties significantly, to up to 10 per cent of group turnover;
- creates incentives to invest in corporate compliance programmes;
- facilitates penalty reductions when an independent internal investigation is conducted and the company in question co-operates with the investigating authorities;
- significantly limits legal privilege (not only for internal investigations);
- offers the alternative of ending proceedings by warning the undertaking, reserving the right to impose penalties and, in some cases, tied to conditions and directives during the period for which such a right is reserved; and
- permits a court to order the appointment of a compliance monitor.

Currently, the draft is still under wraps. It may be passed by the German Bundestag following deliberation by the cabinet and any necessary amendments.

15

Greece

Ilias Anagnostopoulos, Jerina Zapanti and Alexandros Tsagkalidis[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

For the past four years, the Anti-Corruption Prosecutor's Office has been investigating an alleged high-profile corruption case involving a multinational pharmaceutical company. The investigation was initiated when the prosecuting authorities in Greece received knowledge of allegations made by unknown witnesses, who acted as whistleblowers to the authorities in the United States. According to these testimonies, executives of the pharmaceutical company allegedly bribed high-ranking public officials (including politicians) in exchange for securing favourable treatment as regards the price-listing of its products. Moreover, the investigation expanded into alleged bribery schemes involving healthcare professionals to increase the prescription of the pharmaceutical company's products. This has been a highly politicised criminal case, in which politicians (two former prime ministers and former ministers of health) from the major political parties, as well as other individuals, have been openly targeted by the media and officers of the former government.

The Anti-Corruption Prosecutor's Office carried out multiple dawn raids at the company's premises in Athens and seized a large number of documents and laptops. A significant number of witnesses have been examined as well. In parallel, other agencies, such as the Economic and Financial Crime Unit (SDOE) and the Health and Welfare Inspectorate, have been investigating this case. To date, the Prosecutor's Office has not been able to find any evidence to corroborate the whistleblowers' vague allegations, and it has recently dropped the case in respect of the former prime ministers and ministers of health (with the exception of one).

1 Ilias Anagnostopoulos, Jerina Zapanti and Alexandros Tsagkalidis are members of Anagnostopoulos.

Other major investigations have been conducted in relation to multinational companies that have reportedly been systematically giving money to public officials to secure awards of multimillion-euro government contracts, in respect of advanced communication systems, medical supplies and military expenditure (such as Siemens, Johnson & Johnson/DePuy, HDW/Ferrostaal, STN). Investigations have also targeted acts of corruption of former government officials in relation to facilitating payments and tax fraud schemes through real estate deals.

2 Outline the legal framework for corporate liability in your country.

Criminal liability is an exception when referring to a legal entity because, under Greek law, only an individual may be liable for a criminal act. However, harmonisation with international corporate standards, and the need to bring internal legislation in line with European and international instruments, has led to provisions for liability of entities in the form of administrative measures and fines, among others.

Corporate conduct may be punishable in certain cases. Company conduct (e.g., in the context of anti-corruption, anti-money laundering and anti-cartel legislation) is usually punishable when it is linked with positive gains or advantages. The company is liable as an entity – notwithstanding the individual liability of employees – when there is some type of profit, gain or advantage to the company. The severity of punishment in these cases (in the form of administrative penalties or fines) usually depends on the type of profit or gain, and the annual turnover of the company.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The responsibility for the investigation of corporate conduct lies with regulatory and prosecuting authorities (depending on the subject of investigation) but the responsibility for criminal prosecution of corporate conduct always lies with the Prosecutor's Office (the Prosecutor). Regulatory authorities may investigate – within their scope – corporate conduct (e.g., the Competition Commission for cartel offences or the Capital Market Commission for insider dealing or market abuse), and any findings relating to criminal offences are forwarded to the Prosecutor to decide on further proceedings.

It is most common for the SDOE to undertake the necessary preliminary investigations, evidence gathering, reports, and so on, following a prosecutorial order. In cases of money laundering, the Greek Financial Intelligence Unit gathers all necessary information and evidence, and if it believes there is enough to support a criminal case, it forwards the case to the Prosecutor.

The Prosecutor opens a case against the natural person or officers of an entity, following standard criminal procedure, namely conducting a preliminary investigation, filing charges and making a referral to investigation (conducted by an investigating judge). It is not unusual in serious and complex cases (e.g., corruption, large-scale money laundering and fraud) for enforcement agencies and the Prosecutor to take action to secure evidence (by issuing a warrant for search and seizure or issuing freezing orders) before any charges are filed and before persons of interest are called for questioning.

Companies are not criminally prosecuted because they are not criminally liable, but sanctions are imposed against them in the form of administrative penalties for the actions of individuals held liable for criminal acts from which the companies have benefited.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

A preliminary investigation is initiated by the Prosecutor following a *notitia criminis*, namely a criminal complaint (by an individual or entity, usually the victim of a crime) against certain persons, or information submitted to the Prosecutor by another authority, or even information that has come to the knowledge of the Prosecutor through the media or any other sources, and it is usually the very first stage of the proceedings. It is ordered by a prosecutor, unless an agency or enforcement authority may by law gather evidence and information through a preliminary enquiry and submit a request to the Prosecutor for further investigation. All preliminary investigations, apart from regular tax reviews, are supervised by the Prosecutor.

The standard of proof to open a preliminary investigation is low. Even slim evidence of an alleged criminal offence (e.g., unconfirmed press reports or anonymous information) may justify a preliminary investigation.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

The prosecutor or the investigating judge who supervises the investigation should be informed regarding any objections raised against a notice or subpoena. Also, if there is a disagreement between a defendant and the prosecutor or the investigating judge regarding such matters, the validity or lawfulness of a notice or subpoena could be challenged before the Judicial Council, according to the provisions of the Code of Criminal Procedure (CCP).

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Yes. Articles 263A and 187A of the Criminal Code (CC) provide for immunity or leniency for individuals who inform or assist (or both) the prosecuting authorities on corruption cases (263A) or cases involving criminal or terrorist organisations (187A).

7 What are the top priorities for your country's law enforcement authorities?

The detection and prosecution of corruption is one of the main goals of prosecuting and enforcement authorities. Legal provisions in respect of acts of corruption have been amended three times in the past five years to conform with international instruments. Greece has ratified all major EU and international conventions and has passed internal legislation to comply with them. However, continuous amendment of existing legislation creates legal uncertainty and poses complex issues in respect of pending investigations or ongoing trial hearings. More generally, it is apparent that an integrated anti-corruption policy is needed, including better coordination of various legal instruments and anti-corruption agencies.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

In 2016, Greece transposed Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, and replacing Council Framework Decision 2005/222/JHA, and amended its criminal legislation accordingly to strengthen cybersecurity protection; in particular, under the CC, to punish:

- hindering the operation of information systems (Article 292B);
- the supply of hardware or software for the purpose of hindering the operation of information systems (Article 292C);
- unlawful access to an information system (Article 370C);
- unlawful extraction of data from an information system (Article 370D); and
- computer fraud (Article 386A)

The investigation of criminal cases in relation to the above-mentioned crimes is handled by the Cyber Crime Division of the Hellenic Police. After their investigation is finished, they forward the case file to the prosecutors with the court of first instance.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

All regular crimes committed with the use of a computer are punished by Greek law. Special provisions can be found for the crimes of child pornography and attracting children for sexual purposes through information systems (Articles 348A and 348B of the CC). The Cyber Crime Division of the Hellenic Police handles the investigation of cybercrimes as well.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

As a general rule, Greek law does not have extraterritorial effect. Enforcement and sanctions imposed by the Greek authorities are not effective in other jurisdictions unless they meet the requirements of mutual assistance in criminal matters and mutual recognition of judgments through bilateral and multilateral treaties.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border investigations and co-operation with other countries' law enforcement or prosecutorial authorities have become common practice in large-scale investigations. Special law enforcement agencies, such as the SDOE, have entered into agreements with similar agencies in other countries, which has enabled a faster and more efficient exchange of information. Agreements between agencies usually follow framework agreements or treaties between countries. In the case of Greece, most aspects of international co-operation are treaty-based. There

are two sets of rules applicable to this prosecutorial co-operation, one of which applies to co-operation with Member States of the European Union (in these cases, all procedures and functions are simplified and faster). In all other cases, provisions for mutual assistance apply (for investigating acts or requests for information).

Greek legislation has undergone a series of amendments to fully comply with international treaties and the obligations arising from Greece's participation in international organisations, among others. However, the introduction of new legislation and measures not totally compatible with existing procedures and practices has prevented a smooth integration of new measures with traditional prosecutorial and investigative practices. Also, efforts to adjust legislation to international instruments as much as possible (especially in combating corruption and money laundering) have led, in many instances, to the powers of different law enforcement agencies overlapping, and there is no general rule or central authority to resolve such issues or to propose any necessary adjustments.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The rules of double jeopardy, or *ne bis in idem*, are not directly applicable to entities as they are not the subject of a criminal prosecution. These rules may be indirectly applied (through examination of individual criminal liability) but this is a disputed matter.

13 Are 'global' settlements common in your country? What are the practical considerations?

No. In certain cases, Greece has entered into a settlement in the context of ad hoc agreements with the companies under investigation. These types of settlements do not cover the criminal liability of individuals, such as directors or employees of the company.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Foreign decisions are usually taken into account by Greek courts in relation to the findings regarding the merits of the case, but they do not bar Greek proceedings from advancing. The Greek state, in practice, applies its law to companies for conduct within the country or for acts that have effects within the country. In this respect, Greek authorities seek to impose the law on companies either registered in Greece or active in the Greek economy (e.g., companies with registered offices in other countries that have agencies or subsidiaries in Greece).

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Greece does not have its own sanctions programme but sanctions are imposed through EU Regulations, which are directly applicable, and by UN Resolutions, which are implemented by Presidential Decrees.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

See question 15.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

As regards the freezing and unfreezing of assets of states, legal persons, legal entities or natural persons imposed by UN Security Council resolutions, UN decisions or pursuant to EU Regulations or Decisions, for any legitimate reason under international law, the competent authority is Unit B of the Hellenic Financial Intelligence Unit. As regards restrictions on imports and exports, the competent authority is the General Directorate of International Economic Policy, Directorate of Import-Export Regimes and Trade Instruments of the Ministry of Development and Competitiveness. These authorities often liaise, coordinate and communicate with their foreign counterparts to exchange information.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Council Regulation (EC) No. 2271/96 (known as the Blocking Regulation) is directly applicable in Greece.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

See question 18.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of corporate misconduct most often come to light through investigations conducted by regulatory agencies such as the Competition Commission, the Capital Market Commission and the Financial Intelligence Unit in respect of breaches of regulations within their competence. The authorities regularly receive related information (officially and unofficially) from a number of sources, including whistleblowers. Self-reporting by companies is still rather unusual.

Information gathering

21 Does your country have a data protection regime?

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation), which came into effect in May 2018. Legislation is currently being drafted to implement the Regulation.
- Law 2472/1997: Protection of Individuals with regard to the Processing of Personal Data.
- Law 3471/2006: Protection of personal data and privacy in the electronic telecommunications sector and amendment of Law 2472/1997.
- By-laws issued by the Hellenic Data Protection Authority (HDPA).

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The HDPA is a constitutionally independent administrative authority that supervises the application of data protection laws and regulations, and imposes administrative sanctions on natural or legal persons who violate those laws. The primary mission of the HDPA is the protection of individuals from the unlawful processing of their personal data and providing assistance if it is established that an individual's rights have been violated in any sector (such as financial, health, insurance, education, public administration, transport or mass media).

Moreover, criminal sanctions may be imposed by the courts on persons who violate data protection legislation.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

Internal investigations are not regulated by special legal provisions, so the general rules concerning data protection and privileges apply. As a general rule, employees must be loyal to the company they serve, handle sensitive information with care and avoid activities conflicting with the company's interests. On the other hand, the company, as an employer, must respect and protect sensitive personal information about its employees and any personal communications.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

It is common practice, also recognised by the Greek courts, for an employer to have access to its employees' business communications, such as emails, calls or text messages circulated through the company's communication infrastructure (servers, backup storage, etc.). In most cases, this type of access is provided for in the company's internal work regulations and is agreed by both parties in the employment contract.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

In the majority of cases, the authorities will send a written request to a company to provide certain information or documents. In principle, a company must co-operate with the authorities, at least in terms of providing requested information and documentation. Failure to comply with such a request usually has no direct consequences (unless otherwise provided for by law) but may lead to an unfavourable report by the authorities or an on-site search and seizure to obtain requested material.

In all cases, the company may object to handing over certain documents or material (e.g., privileged commercial information or correspondence) and refer to the Prosecutor to resolve the issue. In practice, when an on-site search is in progress, the company may not refuse to hand over material but may raise its objections regarding the nature of the material taken (e.g., privileged information) when signing the confiscation documents, in which case the material is sealed and taken by the agency, pending resolution of the issue by the courts.

On some occasions (depending on the scope and nature of an investigation), the company may be requested to submit its views in respect of the issues under investigation or to offer evidence in its defence (of any type: witnesses, bank records, correspondence, among others) contesting the views of the investigating authority (usually included in a draft report).

Dawn raids may take place in emergency situations (to secure evidence, for instance) and home searches are conducted in the presence of a prosecutor or magistrate.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

According to Article 212 of the CCP, information in the possession of clerics, lawyers, doctors, pharmacists and military diplomatic officials is considered privileged. During a search of its premises, a company may declare that certain documents are privileged information pursuant to Article 212 of the CCP. If the investigating authority contests this assertion, it will confiscate the documents, seal them without acquiring knowledge of their content and request the competent professional association to decide on the confidentiality of the seized documents. The general rule is that documents containing privileged information may not be included in the confiscated documents. This restriction is not applicable when the person protected by privilege (such as a lawyer, doctor or cleric) is under investigation as an accomplice in a criminal act. Personal documents of employees are protected to a certain extent, depending on the specifics of the case.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

All authorities with the power to conduct investigations in their field (e.g., the Prosecutor, the police, the Financial and Economic Crime Unit, the Capital Market Commission) may

request that individuals give statements following an order by the Prosecutor or in accordance with specific legal provisions. In cases of serious business crimes, the Prosecutor usually orders a specific person to give a statement either as a witness or as a suspect (witness under caution) while the actual questioning is most commonly conducted by the police or the Financial and Economic Crime Unit (which is an agency supervised by the Ministry of Finance and has powers similar to the police, such as conducting investigations, examining witnesses and performing on-site inspections).

If an individual is called as a witness, he or she appears before the authority that has received the Prosecutor's order and gives a statement under oath. Persons called as witnesses to provide testimony must appear before the authority that conducts the investigation to answer the questions. Witnesses have the right to avoid self-incrimination.

Individuals called as suspects have the right to request copies of the case file and sufficient time to prepare for questioning. At this preliminary stage, suspects are also entitled to a defence attorney, who may be present during questioning, and to file written submissions in their defence.

In all cases where questioning of individuals as suspects is involved, relevant provisions of the CCP apply, namely the right to avoid self-incrimination, the right to an attorney, time to prepare one's defence, the right to remain silent, and so on. The structure of pretrial procedure is such that a suspect may have full representation by a defence attorney and full protection of his or her rights.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Greece does not have systematic legislation protecting whistleblowers in either the public or the private sector, nor does it have any relevant financial incentive schemes. Whistleblowers may be considered as witnesses in the public interest, which results in complete protection from criminal prosecution with respect to offences such as disclosure of privileged information or filing a false complaint relating to the information the whistleblower provides to the authorities, according to Article 47 of the CCP.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Local employment law does not grant special rights to employees who are under investigation, nor does it distinguish between officers and directors. Nevertheless, employees must be treated with respect, and the investigation should be conducted in accordance with data protection and labour laws.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

In cases of alleged serious misconduct, both employees and directors are usually notified in case the individual wishes to have counsel present at interviews; it is for the individual to decide on the presence of counsel.

A company's policy in cases of individual liability will depend on the type of misconduct (negligent or deliberate), the seriousness of the actions, the position of the individual, among other things. It is customary for a company to collaborate with an individual's counsel when the action occurred as a result of his or her position in the company (e.g., administrative proceedings or criminal proceedings against a managing director for an environmental offence).

Termination of an employee's contract is something that the company has to decide on after reviewing the whole case and assessing possible consequences for the entity. If the employee has acted against the company's best interests and the actions are the reason the government seeks to impose liability, the company may have no option but to terminate the contract to protect its interests, privileged information, and so on. In the end, it is a strategic decision for the company unless the particulars of the case leave no option other than to terminate the employment. This is especially the case when an employee is involved in large-scale or serious violations of duties, has deliberately acted against the company's interests, or engaged in fraudulent activity against the company itself, its clients or the general public.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

The obligation of an employee to participate in an internal investigation depends on the terms of the employment contract and the applicable law. Refusal to participate in internal proceedings could eventually lead to dismissal.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

No special statutory rules regulate internal investigations. Thus, the way in which internal investigations are conducted varies. Usually, the department of a company that is to conduct the investigation decides how to proceed.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There is no general rule or obligation for self-reporting. A series of legislative measures have been passed to enable enforcement agencies to detect misconduct with or without the

co-operation of the companies. In this respect, accounting officers must report any suspicious activity (relating to tax evasion, money laundering and the like) if there are indications of misconduct.

However, there are special provisions in numerous laws and regulations that stipulate self-reporting of internal wrongdoing and cover most aspects of business activity. In some fields or industries, provisions for self-reporting are more stringent (e.g., banking and financial services), while in others there is no explicit provision for self-reporting (most commercial activities in the private sector); however, rules for reporting criminal acts to the authorities (as a general legal obligation) may apply and this might, to some extent, lead to some kind of self-reporting.

There are specific industries or fields in which self-reporting is a prerequisite to obtaining the benefit of leniency measures or for immunity provisions to apply in cases of violations of competition law, exposure of corrupt practices of public officials, organised crime and terrorism.

In any of these procedures, the authorities can choose to impose lesser penalties or grant complete immunity. These provisions may apply to corporate entities only, to individuals only, or to entities and individuals alike. Considering that, in the majority of cases involving serious corporate misconduct, the authorities may impose administrative penalties and measures affecting the company's ability to continue and develop its activities, as a rule, participation in a leniency programme is considered the better option for a company and the implicated individuals.

Where leniency or immunity measures are provided for (e.g., cartel offences, corrupt practices or money laundering), the extent to which they apply depends on the type of information provided to the authorities. As a rule, effective and complete exposure of illegal practices may lead to lesser penalties or immunity from criminal prosecution or administrative sanctions. Immunity would usually be granted when the reporting of illegal practices is of such significance that it contributes substantially to the exposure of illegal activity or perpetrators.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

- Notify the legal department regarding the nature of the notice or subpoena and consult on how to proceed next.
- Retrieve any requested documents or data.
- Evaluate the possible implications from a criminal and an administrative perspective in relation to the requested documents or data.
- Decide whether and how to comply with the request.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

No general obligation is provided for by Greek law, but in certain fields (e.g., competition regulation), corporations are given motives for self-reporting through provisions for leniency or immunity programmes, or both. Listed companies must disclose relevant information to the public in accordance with the existing regulations.

36 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are welcomed by the law authorities, when they are conducted in a manner that leads to direct gathering of evidence, preservation and referral of evidence to the authorities. However, the absence of a clear legal framework for regulating internal investigations poses complex issues in relation to the protection of affected individuals.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Attorney–client privilege may be asserted at any time. However, it is not always easy to determine what falls under this protection. Apart from the obvious privileged information (such as correspondence between an attorney and a client), there are other forms of communication (e.g., memos, drafts of letters or other documented material) that may contain privileged information.

The company is not expected to waive its rights or privileges (especially attorney–client privilege) as part of its co-operation with the authorities. However, the company may choose to waive its rights in whole or in part with respect to such privileges if it becomes necessary for the purposes of its defence in regulatory or criminal procedures. For documents and material protected by special legislation (e.g., patents), the company is entitled to deny access, give limited access or request that the material be handled by the competent authorities in accordance with special legal provisions.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Attorney–client privilege is considered to be of paramount importance and is well established in Greek legislation. Sources of this privilege are to be found in the Lawyer's Code of Conduct, the CCP, the Criminal Code and the Code of Civil Procedure. Attorney–client privilege is broad and covers any type of data (verbal, written, electronic, etc.) obtained from the client, regardless of whether the client is a natural or legal person. Attorney–client privilege may be invoked even after the termination of the relationship between an attorney and a client.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes. In Greek law there is no distinction between in-house and external counsel in this respect.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

No. In principle, it applies to lawyers registered in Greece.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Waiving the attorney–client privilege is not common practice in the legal system and is not provided for as a mandatory or required step in any context.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

When a company is requested by the authorities to produce privileged information (and has decided to comply with the request), it is common practice to provide limited information relating only to the scope of the request. However, no effective safeguards are in place as to how the information provided could be used by third parties, including other authorities and agencies.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Yes. Waiver of privilege is valid only when it is conducted according to the provisions of Greek law.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

There is no special rule regarding common interest privilege. It falls under the attorney–client privilege.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

There is no explicit legal provision or relevant case law covering this matter. Privilege can be claimed regarding the documents in the lawyer's possession. However, it is doubtful whether privilege would apply to communications between lawyers and third parties or in relation to documents in the possession of third parties.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Yes.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

See questions 36 and 29. Third parties are not obliged to testify as witnesses in corporate internal proceedings.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

There is no established protocol for conducting internal interviews of witnesses. It is usually decided by the department within the company that is to conduct the investigation, which also decides on the strategy of the questioning and whether documents will be put to the witnesses. In cases of alleged serious misconduct, the employee is usually notified in case he or she wishes to have counsel present; it is for the employee to decide on the presence of counsel.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

A business may conduct its own internal investigation on any occasion. Whether the results should be shared with the authorities depends on the results and the nature of the case, since there is no general rule for self-reporting – with the exception of certain aspects of business activities usually related to regulatory rather than criminal provisions.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

If there is evidence of serious wrongdoing, the company may be left with no choice but to refer all gathered information to the authorities. It is important to keep in mind on all occasions that any report to the authorities by the company, especially in relation to its employees or clients, should be done carefully to avoid any possibility of it being held liable for filing false accusations. It is not expected, of course, that a case be presented to the authorities proven beyond any doubt, but care should be taken to forward information that indicates with some certainty that serious misconduct has taken place.

Self-reporting may extend to third countries, when there is favourable legislation regarding self-reporting from which the company could benefit (e.g., if the company could reach a leniency or immunity agreement under certain conditions).

52 What are the practical steps you need to take to self-report to law enforcement in your country?

The first step is to gather and secure all evidence regarding the alleged wrongdoing. Next, a detailed report should be drafted, to explain, with some certainty, that serious misconduct has taken place. Finally, the report is filed with the Prosecutor or other competent authority.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

In principle, a company must co-operate with the authorities, at least in terms of providing requested information and documentation. Failure to comply with such a request usually has no direct consequences (unless otherwise provided for by law) but may lead to an unfavourable report by the authorities or an on-site search and seizure to obtain the requested material.

In practice, a company's attorney (in-house counsel or an independent attorney) liaises with the authorities and informs them whether or not the company will comply with the notice or subpoena, and requests additional information regarding the scope of the investigation and its purpose.

54 Are ongoing authority investigations subject to challenge before the courts?

Although it is not common, the validity of investigative actions, such as searches and seizures, may be challenged before the Judicial Council, according to the provisions of the CCP.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

When multiple jurisdictions are involved, an international instrument or treaty may be applicable in the first instance. If the relevant jurisdictions are all EU Member States, EU law is applied; this is very similar to Greek law on the basic elements of procedure. If a bilateral or international treaty is in force (in relation to other countries), the provisions of the treaty are primarily applied. Treaties usually have specific provisions on how to handle privileged information or private data but, in some cases, Greece reserves the right to refuse to forward requested information if it is against Greek law, or may reserve the right to forward it subject to approval from the competent authority (e.g., dealing with protection of private data).

In large-scale investigations involving more jurisdictions, all investigations are usually carried out locally in accordance with Greek law and regulations. Exceptions may apply in cases involving national security or relating to Greece's diplomatic relations, in which case different rules (as set out in international or bilateral treaties) may apply.

A company can always notify the authorities in different jurisdictions of a current investigation in Greece, to avoid multiple prosecutions or sanctions and a potential breach of the *ne bis in idem* principle.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

See question 55.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Co-operation with other countries' law enforcement or prosecutorial authorities has become common practice in large-scale investigations. Special law enforcement agencies, such as the SDOE, have entered into agreements with foreign counterparts, which has enabled a faster and more efficient exchange of information. Agreements between agencies usually follow framework agreements or treaties between countries. In the case of Greece, most aspects of international co-operation are treaty-based.

In recent times, there has been a marked increase in the co-operation of special prosecuting and investigating task forces with the corresponding authorities in other countries (especially in Germany and Switzerland) by adopting more flexible and quicker procedures.

There are two sets of rules applicable to this prosecutorial co-operation, one of which applies to co-operation with EU Member States (in these cases, all procedures and functions are simplified and faster). In all other cases, provisions for mutual assistance apply (for investigating acts or requests for information).

Greece is party to numerous international and European conventions and bilateral agreements covering all aspects of cross-border judicial co-operation, such as:

- the European Convention on Mutual Assistance in Criminal Matters (1959);
- the European Convention on the suppression of terrorism (1977);
- the Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990);
- the UN Convention against Transnational Organized Crime (2000);
- the UN Convention against Corruption (2003);
- the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (2005); and
- bilateral agreements with the United States, China, Poland, Mexico and other countries.

Greek courts co-operate with those of other EU Member States through the Eurojust agency.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Under the Greek Code of Criminal Procedure, investigation proceedings are confidential and this confidentiality applies to all information gathered by the enforcement authorities. Only the person under investigation and the authorities have access to this information. Information gathered is not disclosed to third parties unless they have a specific legitimate interest to obtain such information, following special authorisation by the prosecuting authorities.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The company should inform the Greek authorities that complying with such a request would be illegal under the laws of that third country. Thus, the Greek authorities would

decide whether to obtain the evidence through official channels (such as filing a request for mutual assistance).

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

According to Article 212 of the CCP, information in the possession of clerics, lawyers, doctors, pharmacists and military diplomatic officials is considered privileged. If an individual under investigation declares that certain documents are privileged information pursuant to Article 212 of the CCP and the investigating authority contests this assertion, the documents confiscated are sealed, without the latter acquiring knowledge of their content, and a request is submitted to the competent professional association to decide on the confidentiality of the documents.

This restriction does not apply if the person protected by privilege is under investigation as an accomplice to a criminal act.

Data protection statutes (Law 2472/1997) are not applicable in criminal proceedings.

In criminal proceedings, as opposed to administrative or tax proceedings, there is no general legal framework governing the co-operation of a private legal entity with the investigating authorities (except when explicitly stated by law). In this respect, companies are not obliged to carry out the investigating authorities' requests for providing evidence, unless stated otherwise by law (e.g., telecommunications companies are obliged to provide data, when requested by a prosecutor or the investigating judge). However, 'passive' co-operation is expected when searches are conducted at the premises of companies; in other words, a company is not allowed actively to hinder searches conducted at its offices, such as by destroying evidence.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

As a general rule, material requested by the prosecuting authorities during the conduct of a criminal investigation must be produced. If part of this material contains privileged information, there are procedures under the CCP for handling this information accordingly. Most privileges do not apply in investigations into corruption. The Anti-Corruption Prosecutor, the Financial Crime Prosecutor and certain agencies, such as the SDOE, may have full access to most of the privileged information. Production of material by third parties is also taken into consideration if they have legal access to it and it is not gathered or accessed through violation of criminal provisions (e.g., illegal recording of conversations or illegal access to personal data).

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Depending on the nature of the misconduct, a broad variety of administrative sanctions may be imposed against a company, such as fines, licence revocation, a permanent or temporary ban from public tenders or state funding, or a temporary suspension of the business operations of the company.

Individuals may face criminal penalties (which may include imprisonment and monetary penalties) if they are found guilty of a criminal offence.

It should be noted that crimes relating to an entity may be committed by members of the entity, mainly managers, officers and directors. These individuals are personally liable in any case, but they cannot be held liable for criminal acts 'committed' by the entity if they do not meet the criteria (objective and subjective) of the relevant legal provision. For some types of offences (e.g., tax offences), there are special provisions as to which persons are deemed liable under the relevant law. These legal provisions may expand or restrict liability to individuals holding certain positions within an entity.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Suspension and debarment of a company from government contracts in Greece is an administrative penalty that can be found in various laws:

- According to Article 45 of Law 4557/2018 regarding money laundering, failure to comply with the Law's anti-money laundering provisions may lead to the corporation being prohibited from carrying out certain activities, establishing new branches in Greece or abroad, or increasing its share capital. In the case of serious or repeated violations, failure to comply may result in final or provisional withdrawal or suspension of authorisation of the corporation for a specific time or prohibition from carrying out its business.
- According to Article 28, Paragraph 5 of Law 1650/1986 (as amended by Article 7, Paragraph 4 of Law 4042/2012) regarding the protection of the environment, a company may be banned temporarily or permanently from public tenders if it is found liable for polluting or degrading the environment to gain illicit profits.
- According to Article 24 of Law 3340/2005 for the protection of the capital market from actions of persons that possess inside information and market manipulation, the activities of a company found to be violating the provisions of that Law may be suspended.

The company should primarily examine whether the intended settlement in another country concerns facts that have taken place in Greece and evaluate the risk of that settlement being used in future proceedings in Greece.

64 What do the authorities in your country take into account when fixing penalties?

When imposing sanctions (in the form of administrative penalties) on a corporation, the competent authorities consider the following factors: entity size and annual turnover,

seriousness of the offence, damage caused, the amount by which the company benefited from the conduct and prior misconduct. The fine is imposed by the relevant competent authority (usually the Revenue Service). Apart from a fine, the competent authority may impose additional measures, such as prohibition of business activity for a specified period, revocation of licences and registrations, a ban from public tenders or investment programmes, etc. Judicial control of sanctions is always available to affected parties.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

No. However, alternative forms for the resolution of criminal cases involving individuals were recently introduced into the CCP.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

No.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Prior to any settlement with a law enforcement authority, a company should consider whether the settlement agreement could be used as evidence against individuals (i.e., directors or employees of the company) or even against the company itself in any type of proceeding (i.e., criminal, administrative or civil). Also, the company should thoroughly negotiate with the authorities the wording of the settlement agreement to avoid any indirect admission of wrongdoing that is not covered by that agreement.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Regulatory agencies (such as the Competition Commission, the Capital Market Commission and the Greek Gaming Commission) monitor the adherence of corporate entities to standards set by the relevant legal provisions in respect to matters within their competence. In the case of breaches, these agencies have the powers to pose administrative penalties and to forward their findings to the Prosecutor's Office for a criminal investigation to be initiated.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Yes, private actions seeking damages in the course of civil proceedings are allowed. Private plaintiffs may gain access to authorities' files, provided that they can adequately prove their legitimate interest in obtaining the files to support their civil claims against the company.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

According to Article 241 of the CCP, the pretrial stage of the proceedings, which includes the preliminary inquiry and the main investigation, is conducted in secrecy, not publicly. However, in highly publicised cases, it is not unusual that information (including, inter alia, documentary evidence, witness statements) is leaked to the media during the investigation phase.

After a case has been referred for trial, all procedures, including the trial hearing, are, as a rule, in the public domain, according to Article 329 of the CCP.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

There is no standard corporate communication protocol in Greece, thus companies would usually follow the international standards regarding communications in crisis management. However, it is common for companies to have their own public communications and media department. In some cases, companies also use public relations firms to manage a corporate crisis.

72 How is publicity managed when there are ongoing related proceedings?

Companies decide on how to manage publicity case by case. Crucial factors that help to develop a company's strategy are the nature of the proceedings and the company's involvement regarding the facts under investigation and the investigated persons.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

No, but it may be advisable in some circumstances.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

No.

16

Hong Kong

Donna Wacker, Wendy Wysong, Anita Lam, William Wong, Michael Wang and Nicholas Turner[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The Hong Kong Securities and Futures Commission (SFC) remains active in pursuing alleged corporate misfeasance among listed companies, as well as members of their current or former senior management. It works closely with the Independent Commission Against Corruption (ICAC). Following a joint operation with the SFC, in May and July 2019, the ICAC charged a number of former executive directors and managers of Convoy Global Holdings Limited with conspiracy to defraud. In June 2019, the SFC and the ICAC mounted another joint operation and searched the offices of two sponsor firms, two listed companies and a financial printing company. The ICAC arrested a former joint head of the Initial Public Offering Vetting Team of the Listing Department of the Hong Kong Exchanges and Clearing Limited and two of his associates.

Another notable feature is the close co-operation between the SFC and the Mainland Chinese regulators, including the China Securities Regulatory Commission (CSRC) and the China Banking Regulatory Commission. In late 2017, the SFC and the CSRC carried out a joint investigation into an individual (Tang Hanbo) for stock manipulation through the China-Hong Kong Stock Connect programme, leading to administrative penalties imposed by the CSRC and the criminal conviction of Tang in China.

1 Donna Wacker is a partner, Wendy Wysong is a foreign legal consultant (Hong Kong) and a partner (Washington, DC), Anita Lam and William Wong are consultants, Michael Wang is a senior associate and Nicholas Turner is a registered foreign lawyer at Clifford Chance.

2 Outline the legal framework for corporate liability in your country.

The law of Hong Kong has followed the common law of England and Wales in ascribing corporate liability for criminality, and has developed two main techniques for attributing to a corporate the acts and states of mind of the individuals it employs:

- the 'identification principle', whereby, subject to some limited exceptions, a corporate entity may be indicted and convicted for the criminal acts of the directors and managers who represent its directing mind and will, and who control what it does; and
- vicarious liability, under which a corporation is liable for the criminal acts of its employees or agents under statutory offences that impose an absolute duty on the employer.

A number of offences in Hong Kong legislation target corporates and regulate business activity. They include offences provided in the Companies Ordinance, the Securities and Futures Ordinance (SFO), the Trade Descriptions Ordinance and the Theft Ordinance.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Corporations are subject to investigation or regulation by a number of authorities, including the ICAC, the Hong Kong Police Force (HKPF), the Customs and Excise Department, the Companies Registry, the Inland Revenue Department, the SFC, the Hong Kong Monetary Authority (HKMA), the Insurance Authority (IA), the Competition Commission and the Office of the Privacy Commissioner (OPC).

Hong Kong's Department of Justice (DOJ) has overall responsibility for conducting criminal prosecutions; the other authorities named above conduct investigations and sometimes carry out prosecutions, depending on the offences involved. There has been an increase in co-operation between law enforcement authorities in mounting joint investigations into suspected misfeasance by listed companies and their directors and officers. See, as an example, the joint operations by the SFC and the ICAC described in question 1.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

In general, criminal authorities must have reasonable grounds to suspect that a crime has been committed before starting an investigation. The threshold of suspicion is relatively low.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A challenge to a search and seizure warrant or production order, and a request to exclude evidence gathered as a result, can be made based on scope, the grounds on which the order was obtained, legal professional privilege or public interest grounds through an application to the Hong Kong courts.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Deferred prosecution agreements (DPAs) are commonly used by prosecutors and regulators in the United States and the United Kingdom. Although they have not been formally introduced in Hong Kong, different Hong Kong regulators have, in practice, their own co-operation arrangements. For example, the ICAC or the HKPF from time to time grant perpetrators immunity from prosecution in return for co-operation, after consultation with the DOJ. Both the SFC and the HKMA have published guidance notes on co-operation in investigations and enforcement proceedings under which a person may obtain a credit on the disciplinary penalty if they settle with the regulators. These guidance notes do not apply to criminal cases over which the DOJ has sole discretion. It is also common for the SFC or the HKMA to require, as a part of a settlement, the appointment of an independent reviewer, which may perform a role similar to a that of a monitor under DPAs in the United States or the United Kingdom.

7 What are the top priorities for your country's law enforcement authorities?

The HKPF's priorities are violent crime and domestic violence, triads, syndicated and organised crime, dangerous drugs, public safety and the prevention of terrorism. The HKPF is also prioritising cybersecurity and technology crime, particularly criminal groups engaged in internet and telephone fraud.

The SFC's enforcement priorities include corporate misfeasance and fraud by listed companies or senior management, insider dealing and market manipulation, intermediary misconduct and money laundering.

The HKMA's work priorities include risk management relating to operational resilience and technology, money laundering and terrorist financing, misconduct, liquidity and market risk management, and credit.

The IA focuses on protecting and promoting the rights and interests of policyholders and facilitating the sustainable development of the insurance industry both in Hong Kong and regionally. Starting from 23 September 2019, the IA has delegated certain inspection and investigation powers to the HKMA with respect to insurance-related businesses carried on by authorised institutions.

The ICAC has announced a focus on corruption occurring in connection with the Belt and Road Initiative and helping other countries to strengthen their anti-corruption capabilities. It continues to ensure public sector integrity and to investigate cases that violate the common law offence of misconduct in public office.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

There is no overarching legal framework for cybersecurity in Hong Kong. Entities regulated by the HKMA and the SFC must abide by the regulatory guidance issued, including the various guidelines and circulars concerning cyber risk management, resilience testing and

management accountability. The Personal Data Privacy Ordinance (PDPO) addresses the security of personal data, including data storage and security measures.

Large-scale cybersecurity failings resulting in breach of personal data protection rules are treated seriously by regulators. The OPC regularly carries out investigations of such failings and issues enforcement notices, which, if not complied with, may lead to criminal sanctions.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

There are a number of offences under Hong Kong law targeting cybersecurity-related crimes, including unauthorised access to a computer by telecommunications under the Telecommunications Ordinance and access to a computer with criminal or dishonest intent under the Crimes Ordinance. Other offences that may be applied to prosecute cybercrime include criminal damage under the Crimes Ordinance and theft under the Theft Ordinance.

The Cybersecurity and Technology Crime Bureau (CSTCB) of the HKPF is responsible for handling cybersecurity issues, carrying out investigations into technology crime and computer forensic examinations, and the prevention of technology crime. The CSTCB also liaises closely with local and overseas law enforcement agencies for combating cross-border technology crime and to exchange experience.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

The primary basis of criminal jurisdiction in Hong Kong is territorial, and the courts apply a strong presumption against construing statutes as having extraterritorial effect.

The Criminal Jurisdiction Ordinance (CJO) deals with Hong Kong's extraterritorial criminal jurisdiction. The offences to which the CJO applies are divided into Group A offences, which include theft, fraud, deception, blackmail and offences relating to false instruments, and Group B offences, which cover conspiracy, attempting or incitement to commit a Group A offence, and the offence of conspiracy to defraud.

The CJO allows Hong Kong courts to exercise jurisdiction over offences under Groups A and B in the following circumstances:

- any one of the constituent elements of the offence occurs in Hong Kong;
- there is an attempt to commit the offence in Hong Kong, whether or not the attempt is made in Hong Kong or elsewhere and irrespective of whether it has an effect in Hong Kong;
- there is an attempt or incitement in Hong Kong to commit the offence outside Hong Kong; and
- the substantive offence was not intended to take place in Hong Kong.

As regards a conspiracy to commit a Group A offence, or conspiracy to defraud, jurisdiction depends on proof that the pursuit of the agreed course of conduct would involve conduct

punishable under the law in force in the place where the conduct was intended to take place. The prosecution must also prove that:

- a party to the agreement constituting the conspiracy, or a party's agent, did something in Hong Kong in relation to the agreement before its formation;
- a party to the conspiracy became a party in Hong Kong (by joining it either in person or through an agent); or
- a party to the conspiracy, or a party's agent, did or omitted to do anything in Hong Kong in pursuance of it; and
- the conspiracy would be triable in Hong Kong, but the parties to it had not intended that the offence or fraud would take place in Hong Kong.

In relation to conspiracies to commit all other offences, section 159A of the Crimes Ordinance codifies the general common law rule limiting extraterritorial jurisdiction in conspiracy cases and provides that conspiracies entered into in Hong Kong are triable in Hong Kong only if the agreement is to commit substantive offences triable in Hong Kong. Conspiracies entered into abroad to commit substantive offences in Hong Kong would be triable in Hong Kong even before any acts were carried out in Hong Kong in furtherance of the conspiracies. However, conspiracies entered into in Hong Kong to commit offences abroad would not be triable in Hong Kong.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border investigations may touch upon Hong Kong's data privacy regime, or those of other countries in Asia, such that employee or customer consent may be required prior to disclosing certain protected information. Cross-border investigations involving China should be conducted in compliance with the Chinese Law on Guarding State Secrets and the new Chinese Cybersecurity Law. In certain cases, investigators may need to undertake their work on site in China with strict protocols in place to prevent the prohibited export of information to Hong Kong or elsewhere.

In July 2019, the Chinese Ministry of Finance (MOF), the CSRC and the SFC entered into a memorandum of understanding concerning the obtaining of audit working papers in China. The aim of this is to facilitate the SFC's access to these documents when conducting investigations into Chinese companies listed in Hong Kong and their related entities or persons. Under the memorandum of understanding, the MOF and the CSRC will provide the fullest assistance in response to requests by the SFC for investigative assistance regarding the provision of audit working papers.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The right of an accused to advance double jeopardy is found in the Hong Kong Bill of Rights Ordinance and the Criminal Procedure Ordinance. This protection extends to corporations convicted or acquitted of an offence abroad. There is no express or specific legislation or regulation analogous to the 'anti-piling on' policy as exists in the United States.

13 Are 'global' settlements common in your country? What are the practical considerations?

Generally, settlements involving more than one Hong Kong agency do not occur because one agency will have primacy to resolve the case. There is some uncertainty as to whether this will remain the case with the increased joint operation between law enforcement authorities (see question 1). With regard to global settlements involving more than one country, there are no published figures on their prevalence. The SFC has co-operative arrangements for investigatory assistance and exchange of information with many overseas regulators. In particular, the CSRC and the SFC have maintained a close strategic partnership to tackle cross-border trading misconduct. See, for example, the joint investigation into Tang Hanbo referred to in question 1.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

To facilitate investigation of the same matter, the Hong Kong authorities generally try to co-operate with their counterparts in foreign jurisdictions and in China. For example, in October 2014, the SFC and the CSRC entered into a memorandum of understanding on strengthening cross-boundary regulatory and enforcement co-operation with a view to tackling market manipulation in China and Hong Kong. See also the memorandum of understanding entered into between the MOF, the CSRC and the SFC on audit working papers referred to in question 11.

In addition, Hong Kong has mutual legal assistance agreements with a number of countries, and a number of international treaties provide for cross-border co-operation.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Hong Kong generally adheres to United Nations Security Council sanctions, including pursuant to the Weapons of Mass Destruction (Control of Provisions of Services) Ordinance, the United Nations Sanctions Ordinance and the United Nations (Anti-Terrorism Measures) Ordinance with oversight by the Chinese Ministry of Foreign Affairs. Hong Kong does not

currently impose unilateral or autonomous sanctions. Of note, in June 2018, Hong Kong amended the United Nations Sanctions (Democratic People's Republic of Korea) Regulation to incorporate United Nations Security Council resolutions adopted since December 2014.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Multiple agencies share responsibility for the administration and enforcement of Hong Kong sanctions, including the Chief Executive, the DOJ, the HKMA, the SFC, the Commerce and Economic Development Bureau, the Customs and Excise Department, and the Trade and Industry Department. Although regulatory focus has increased, particularly for the financial sector, there have been no notable cases of criminal enforcement of Hong Kong sanctions in recent years.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Hong Kong has a variety of mutual legal assistance arrangements with foreign jurisdictions, which may be used in support of sanctions-related investigations.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Hong Kong has no such legislation.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Whistleblower complaints, both internal and external, are a frequent source of allegations of misconduct leading to investigations, particularly with respect to bribery and corruption. The ICAC plays a critical role in receiving and investigating complaints made against individuals. Enquiries by the ICAC to companies regarding their employees' conduct will often lead to an internal investigation to identify potential breaches of internal policy even when there is no corporate liability under the law.

Regulatory reviews by the SFC, the HKMA or other regulators are another source of allegations of misconduct. Further, corporations and institutions licensed by the SFC or the HKMA have an obligation to report material breaches (or suspected breaches) of any law, rules or regulations (including suspected misconduct) to their regulators. Specifically, corporations licensed by the SFC are expressly required to report material breaches (or suspected breaches) of market misconduct provisions under the SFO by their clients.

Information gathering

21 Does your country have a data protection regime?

Hong Kong has a data protection regime that has been given statutory force through the PDPO. The PDPO applies to any data relating directly or indirectly to a living person from which it is possible to identify that person and the data is in a form in which access to or processing is practicable. The PDPO contains six data protection principles (DPPs) that govern the purpose and manner of collection, the accuracy and duration of retention, the use and security of personal data, and rights of access and correction.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

Contravening a DPP may give rise to a complaint to be investigated by the OPC. A data user may be punished under the PDPO for failing to comply with an enforcement notice issued by the Privacy Commissioner for Personal Data, after a finding of a contravention. An enforcement notice may direct the data user to take steps to remedy the contravention and prevent a recurrence. A data user may separately bring a civil claim for damages on the basis of a contravention of a DPP, whether or not the Privacy Commissioner has issued an enforcement notice.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

The provisions of the PDPO cover the monitoring and gathering of data in the context of internal investigations, whether this be by monitoring the internet, telephone calls or email. An individual who suffers damage (including 'injured feelings') by reason of a breach may sue.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Interception of communications and covert surveillance are regulated by the Interception of Communications and Surveillance Ordinance and can only be exercised by the Customs and Excise Department, the HKPF and the ICAC with prescribed authorisation.

Monitoring and surveillance of employee communication is regulated by the PDPO. Prior to implementing any surveillance system, the employer must take such steps as are reasonable, in the circumstances, to ensure the employees are aware of (among other things) the fact that the information is being collected and the purpose of collection.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Dawn raids are used by the SFC and the HKMA in the context of regulatory investigations, by the ICAC in bribery investigations and by the HKPF in relation to the commission of

any offence. Dawn raids may also be used by the Competition Commission in investigating offences under the Competition Ordinance. They can take place either with a warrant issued by a magistrate or without a warrant in limited circumstances.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Generally, privileged material cannot be seized during a dawn raid or in response to a search warrant. To protect privileged material from seizure, a claim of privilege should be made, and if there is a dispute as to whether certain material is privileged, the material should be sealed until the dispute is resolved. However, privilege may be overridden by a court order. Privilege will also not attach to material created for the purpose of committing a crime.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Privilege against self-incrimination is recognised in Hong Kong. A person may decline to provide information in an investigation that may lead to self-incrimination.

An exception is that authorities such as the SFC and the HKMA may issue a notice under relevant statutory provisions compelling a witness to answer questions or produce documents, and self-incrimination is not a reason for non-compliance. However, the information provided by the person compelled by the notice will be inadmissible in evidence against the person in criminal proceedings except for certain offences, such as perjury.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Hong Kong currently does not have a comprehensive or overarching framework to protect whistleblowers. There exist no financial incentive schemes for whistleblowers to volunteer information. However, listed companies are encouraged to adopt a whistleblowing policy as 'recommended best practice' under the Hong Kong Exchanges and Clearing Limited Corporate Governance Code. The legal protections for whistleblowers are limited.

Under the Employment Ordinance, an employee giving evidence in proceedings or in response to enquiries in connection with the enforcement of the Employment Ordinance, work accidents or breach of work safety legislation is protected from dismissal and discrimination.

Other ordinances covering race, gender, family status and disability also protect individuals who act against discrimination or assist with investigations against victimisation.

Hong Kong law protects individuals who disclose suspected money laundering or other crimes by preventing the disclosure from being treated as a breach of any restrictions imposed by contract, enactment or rule of conduct.

The Competition Commission in Hong Kong has also published its Leniency Policy, which is designed to encourage companies that may have engaged in illegal activity, such as bid rigging or price-fixing, to report it in exchange for leniency.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employees have limited rights under local employment laws if a company conducts an investigation and may be suspended with pay if the employment contract so provides. An employee may also be suspended without pay in the limited circumstances specified in the Employment Ordinance for generally no more than 14 days. Employees are protected against wrongful, unreasonable or constructive dismissal under local legislation.

Employees have the right to a disciplinary hearing if the company handbook, manual or policy provides for such in relation to employee misconduct. Employees of government or public bodies have the right to a fair hearing.

Executive directors owe additional duties under the Companies Ordinance, the company's articles and common law. In addition to rights they have as an employee of the company, directors also have rights under the Companies Ordinance and articles with respect to the potential threat of removal or disqualification in the case of breach of directors' duties.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

There are no statutory requirements for companies to take disciplinary steps when an employee is suspected of misconduct. However, companies' internal policies and employment contracts may adopt disciplinary procedures for their employees. Companies in regulated industries may be required to suspend or take disciplinary action against employees who carry out regulated activities. Aside from their mandatory obligations, companies may take disciplinary action or steps to investigate misconduct as part of the company's proper internal controls and good corporate governance.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

An employee may potentially be dismissed for refusing to participate in an internal investigation after failing to heed the employer's lawful and reasonable instructions and absent any protected circumstances, such as the employee taking sick leave, maternity leave, paternity leave or work injury leave.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is common practice for an internal investigation to begin with the drafting of an investigation plan detailing the objectives, scope, roles and responsibilities for the investigation. A clearly defined communications plan and the protocol for maintaining legal professional

privilege are also essential from the earliest stages. Increasingly, scoping documents will also identify data custodians and outline procedures for electronic document review.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Depending on the nature of the issue, necessary internal steps could be managed by a company's compliance or legal department in less serious cases, or senior management and the board of directors in the more serious cases. Under the supervision of legal counsel to ensure the protection of legal professional privilege, a company should gather and secure any relevant documents and data, and interview key employees to ensure the continued availability of critical information. Corrective action plans or disciplinary measures should be adopted to address gaps or breaches in compliance controls, which may earn a company mitigation credit in any related enforcement actions.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Ideally, a company should have an established protocol for responding to law enforcement requests, subpoenas or dawn raids, including procedures for the preservation of relevant documents and data. The legal department should issue a preservation notice to all relevant employees immediately upon receiving a law enforcement request, or if it believes that such a request or legal proceedings may be forthcoming. Paper documents and electronic data on servers, laptops, mobile devices or other media should be collected from relevant custodians and logged under the supervision of legal counsel and the company's information technology department. Privileged communications should be segregated and clearly stamped to help prevent accidental disclosure.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

There is no general duty to publicly disclose the existence of an internal investigation or contact from law enforcement (indeed, most agencies impose a secrecy obligation on the subjects of an investigation). The exception is in the case of a listed company when such facts would constitute price-sensitive information, as defined under the SFO, unless exempted or when the SFC has granted a waiver (e.g., in cases involving disclosure restrictions imposed by a foreign government authority). Conversely, there are strict prohibitions against publicly reporting details of investigations by the ICAC for both listed and unlisted companies.

36 How are internal investigations viewed by local enforcement bodies in your country?

In most cases, the authorities recognise the need for, and welcome, at least initial or preliminary internal investigations carried out by corporations. Those corporations licensed by the SFC have a regulatory duty to self-report when there is a material breach (or suspected

breach) by their employees of any rules administered by the SFC, or when there is a material breach (or suspected breach) by their clients of any market misconduct provisions under the SFO. Particular care must be taken to avoid tipping off, whereby corporations are prohibited (except with the authorities' consent) from disclosing the existence of the authorities' investigations to a third party, which may include their employees and their clients.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Legal professional privilege can be claimed over various aspects of an internal investigation.

Case law holds that the whole process of obtaining and giving legal advice should be privileged. Therefore, internal communications (including those between employees of a non-legal function) and materials generated during the information-gathering process of an internal investigation (such as minutes of meetings and interview notes) for the dominant purpose of obtaining and giving legal advice could be privileged. However, legal advice privilege will not attach to communications with, or materials prepared by, a third party (unless the communications or materials are for the dominant purpose of obtaining or seeking legal advice), nor will it cover legal advice given by persons who are not legally qualified (e.g., tax accountants).

During an internal investigation, confidential communications or documents prepared for the dominant purpose of obtaining information or evidence for use in actual or reasonably contemplated litigation – even if the communications are merely for the purpose of establishing facts – will be covered by litigation privilege. To protect privilege, the company should:

- involve lawyers (whether in-house or external counsel) as soon as it is apparent that legal advice is likely to be required;
- avoid creating unnecessary records (where there is no prospect of litigation) that summarise, quote or amend the legal advice received;
- limit circulation of privileged documents on a strictly need-to-know basis;
- manage documents effectively by separating privileged and non-privileged documents; and
- ensure that all documents that are considered to be protected by legal professional privilege are clearly marked 'privileged and confidential'.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Under Hong Kong law, legal professional privilege falls into two categories:

- Legal advice privilege attaches to communications between a client and his or her legal adviser for the purposes of giving and receiving legal advice.
- Litigation privilege attaches to confidential communications between a legal adviser and the client, and to communications between a legal adviser or client and a third party if three conditions are met: litigation is in progress or reasonably in contemplation; the communications are made with the sole or dominant purpose of conducting the actual or anticipated litigation; and the litigation is adversarial, not investigative or inquisitorial.

The privilege belongs to, and can only be waived by, the client and not his or her legal adviser.

In the corporate context, it is advisable to identify the employees authorised to act for the company to seek legal advice for the purposes of claiming legal advice privilege, as English and Hong Kong law have diverged in recent years on this issue.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Legal professional privilege applies equally to in-house and external counsel. However, privilege will only cover communications made by an in-house lawyer acting in a legal (not a managerial) capacity.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Legal professional privilege applies equally to advice sought from foreign lawyers if the advice is given in Hong Kong. If the advice is given from outside Hong Kong, it is possible that privilege can be asserted under Hong Kong law even if the home jurisdiction of the foreign lawyer does not recognise legal professional privilege.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Waiver of legal professional privilege (usually limited) is generally regarded as a sign of co-operation by authorities in a regulatory investigation, although it is not mandatory.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The Court of Appeal has confirmed that a waiver of privilege with regard to one party does not automatically mean that privilege has been waived at large and that privilege is not waived because a privileged document has been disclosed for a limited purpose. The scope of the waiver is determined by the party waiving the privilege. Where privilege is waived for a limited purpose, it is important to ensure that the terms and scope of the limited waiver are clear.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Generally, privilege will not be lost because a privileged document has been disclosed for a limited purpose.

Whether privilege can be maintained if it has been partly waived in another country will depend on a number of factors, including, but not limited to:

- whether the concept of limited or partial waiver is recognised in the country where privilege has been waived;
- the scope and terms of the waiver; and
- whether any statutory provision overrides privilege.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege exists in Hong Kong. Privilege will not be waived if privileged material is disclosed to a third party who shares a common interest in the subject matter of the privileged material. Common interest must exist at the time when the privileged material is disclosed to the third party.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Communications between a third party and the lawyer (or the client) are protected from disclosure by litigation privilege if they are made for the dominant purpose of obtaining information or evidence for use in actual or reasonably contemplated litigation. However, legal advice privilege will generally not apply to communications with third parties (see question 37).

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes. There is no general prohibition under Hong Kong law against interviewing witnesses as part of the information-gathering process in an internal investigation.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Legal advice privilege is often claimed for the records of internal witness interviews. Case law in Hong Kong suggests that a corporation may argue that legal advice privilege exists regarding such records if the interviews are conducted (or the reports are compiled) for the dominant purpose of obtaining and giving legal advice during the internal investigation. This is in contrast to the position in England, for example.

Litigation privilege may only be claimed if it is established that the witness interviews are conducted for the dominant purpose of use in an actual or reasonably contemplated litigation.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Whether the interviewee is an employee or a third party, it is recommended that they be informed that:

- the interview is part of a fact-finding exercise;
- the lawyer conducting the interview represents the company, not the interviewee;
- the interview is protected by legal professional privilege belonging to the company, which can choose to disclose the contents of the interview to third parties, including regulators and authorities, without the interviewee's permission;
- the interviewee may provide personal information covered by data protection laws, which will only be used for the fact-finding or review exercise. This exercise may involve sharing

the interviewee's personal information with other advisers working for the company, regulators and authorities; and
- the contents of the interview are confidential and should not be shared with any other person (including other employees).

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

The internal interview will typically be attended by in-house legal counsel and any specialised investigation team with or without external counsel (depending on the nature and seriousness of the issues involved). Relevant documents are typically put to the witness at the internal interview for reference, comment and explanation, as necessary. There is no legal requirement that employees have their own legal representation at an internal interview, and this is not common in practice.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Generally, a person is under no positive obligation to report crimes or provide assistance to law enforcement authorities, aside from suspicious transaction reports under anti-money laundering laws, which are mandatory, and certain exceptions for licensed corporations and financial institutions.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

While there is no formal arrangement or mechanism for deferred prosecution agreements in Hong Kong, it may be advisable for a company to self-report with a view to demonstrating its proactive and full co-operation with the authorities, which may militate against a decision to prosecute or be considered as a mitigating factor in sentencing.

Whether the self-report should extend to foreign countries will depend on the nature and extent of the issues involved, in particular whether it has a cross-border, regional or global element.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

A company should undertake appropriate internal investigations to ascertain the nature and extent of the issues, and to ensure the contents of any self-report are correct and not misleading (including through any material omission). It should also seek legal advice on the applicable self-reporting obligations.

For licensed corporations and financial institutions that are under a regulatory duty to self-report, a balance needs to be struck between making timely self-reports and ensuring that reports are correct and not misleading.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Hong Kong enforcement agencies, such as the ICAC and the SFC, have extensive powers to compel information to be provided to them by corporations involved in investigations, and there is very little that can be done to challenge requests for information when they are made.

However, it would be unusual for criminal charges to be brought against a corporation without it having an opportunity to discuss the circumstances of the allegations with the enforcement agency. In financial misconduct investigations, the twin regulatory and criminal nature of the supervisory jurisdiction of the SFC and the HKMA means that there would be an opportunity for representations to be made by the corporation, through its lawyers, as to the circumstances, and the proposed remediation, prior to criminal charges being brought.

54 Are ongoing authority investigations subject to challenge before the courts?

The circumstances under which an ongoing investigation could be challenged in the courts are difficult to envisage, short of provable *mala fides* on the part of the enforcement agency.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

These circumstances are most likely to arise in the context of financial regulatory investigations by regulators in different jurisdictions, or international anti-bribery enforcement under the US Foreign Corrupt Practices Act or the Bribery Act in the United Kingdom. In circumstances in which the notices or subpoenas have been validly issued, warrant substantive responses and relate to identical subject matter, it is advisable to adopt consistent disclosure with each agency. Further, assuming that a financial institution's operations are international in nature, coupled with self-reporting obligations imposed in other countries (most notably the United States and the United Kingdom), this usually means that some form of notification or reporting to overseas regulators would be required even in the context of an investigation that primarily concerns Hong Kong, and in the absence of any separate notices or subpoenas being issued by overseas regulators. Given the increasing prevalence of international co-operation between regulators and criminal enforcement agencies, a failure to disclose certain matters in one jurisdiction may well be apparent and seized on as an indication of inadequate compliance or co-operation.

Assuming that the investigation primarily concerns Hong Kong, it is advisable to adopt the disclosure made to the local regulators (e.g., the SFC or the HKMA) as a 'base' document in framing the appropriate disclosure to overseas regulators with reference made to the nexus with other countries (e.g., by reason of the institution's or an individual's licensing status, client impact, and so on). Care should also be taken to ensure that notification has been given to, and in appropriate cases, consent obtained from, the local regulators, before overseas notification or disclosure is made. In particular, the SFC almost always insists that its written

consent be obtained before a licensed corporation can disclose the existence or content of an ongoing investigation, even to an overseas regulator.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Under notices issued by the various Hong Kong enforcement agencies, companies may be required to produce material in their possession, custody, control or power, whether this is located in other countries or solely in Hong Kong, subject to having a reasonable excuse not to do so.

This may give rise to issues in some foreign jurisdictions, where the transmission of certain types of information outside that country may be prohibited by local law. In Hong Kong, exposure to criminal liability under foreign law would not constitute a reasonable excuse for non-compliance with a notice or subpoena. This applies in circumstances where a reasonable person would conclude that the Hong Kong public interest in the investigation of criminal activities outweighs any public or private interest in compliance with the foreign law. However, if there are alternative means of obtaining the documents without materially adverse consequences to the investigation, a real and appreciable risk of prosecution under foreign law would constitute a reasonable excuse for non-compliance.

A related issue arises as to the extent that the company is required to produce relevant material in the possession, custody or power of its parent, subsidiary or an associated company (which may be incorporated in other countries). In general terms, this depends on whether the company subject to investigation (the subject company) has a presently enforceable legal right to obtain the documents from such other companies without the need to obtain the consent of anyone else. This is a question of fact, which depends on whether the subject company has sufficient control over the other companies such that the documents in the possession, custody or power of such other companies can be said to be in fact within the power of the subject company.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Hong Kong regulators, including the HKMA and the SFC, have signed memoranda of understanding to establish co-operative arrangements that include the sharing of information with foreign counterparts, including those in China (see questions 11 and 14). One of the most important of these is the International Organisation of Securities Commissions Multilateral Memorandum of Understanding, which was the first global information-sharing arrangement among securities regulators.

Hong Kong authorities routinely co-operate with their foreign counterparts reciprocally in criminal matters under the framework established in the Mutual Legal Assistance in Criminal Matters Ordinance. However, this particular legislation is not applicable to China, Macao or Taiwan, and there was a failed attempt in June 2019 by the Hong Kong government to expand a modified regime to cover these jurisdictions.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Information provided to enforcement authorities in Hong Kong confidentially during an investigation will remain confidential, except to the extent that its use is necessary within an investigation, prosecution or regulatory enforcement. While it may be shared with other enforcement agencies or regulators under the information-sharing agreements referred to in question 57, it would not be disclosed to other third parties without an order from a court.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

It may be possible to refuse production on the grounds that the foreign illegality constituted a reasonable excuse not to produce the documents under the relevant legislation. However, this would be a difficult argument on which to succeed. These issues should be brought to the attention of the enforcement agency, which should consider whether assistance could be sought under formal channels from the agency in the foreign jurisdiction, to allow the documents to be produced without violating foreign law.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

There are no blocking statutes as such in Hong Kong.

The jurisdiction to order corporations and individuals to provide evidence in aid of foreign proceedings is derived from Part VIII of the Evidence Ordinance. Section 75 of the Evidence Ordinance requires the application to be made pursuant to a 'request issued by or on behalf of a court' outside Hong Kong. In terms of procedure, therefore, a letter of request is required and order 70 of the Rules of the High Court provides the procedural framework for taking evidence or obtaining documents from a Hong Kong entity.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Care must be taken to ensure compliance with a company's confidentiality obligations in relation to information. If disclosure to an authority is voluntary, rather than compelled, then the disclosure may violate these obligations.

Law enforcement authorities in Hong Kong must maintain the confidentiality of confidential disclosures made to them (whether voluntary or compelled), except to the extent that they choose to share them with other enforcement authorities, or use the information in an investigation, prosecution or regulatory enforcement action.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Companies or their directors, officers or employees may face disciplinary action – and, in the case of directors, disqualification – and attract potential civil or criminal liability for misconduct in Hong Kong. For entities regulated by the SFC, misconduct would include breaches of the SFO, contravention of the terms of any SFC licence or any act prejudicial to the public interest. Sanctions may include a private or public reprimand, a fine of up to HK$10 million or three times the profit gained or loss avoided, revocation or suspension of licences or registrations, and a ban on regulated persons from applying to be licensed or approved as a responsible officer.

The SFC has powers under the SFO to seek criminal prosecution by the DOJ and, in practice, the SFC refers all market misconduct cases to the DOJ for advice. The maximum penalties for a person convicted of a market misconduct offence are imprisonment for 10 years and a fine of HK$10 million.

The SFC may also institute civil proceedings before the High Court or the Market Misconduct Tribunal (MMT).

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

It depends on the laws of the other country in which the corporate wants to settle. The risk of a corporate's suspension, debarment or other restrictions on continuing business in Hong Kong does not, as a matter of Hong Kong law, restrict the corporate from settling in another country; however, there may be legal requirements in that other country (e.g., disclosure obligations) that allow a regulator or law enforcement agency in that country to reopen a settlement if it subsequently discovers the restrictions on the corporate in Hong Kong of which it has not been previously informed.

64 What do the authorities in your country take into account when fixing penalties?

The authorities will consider all the circumstances of the case, including (1) the nature and seriousness of the conduct, (2) the value of profits accrued or loss avoided, (3) other circumstances of the firm or individual, and (4) other relevant factors.

In considering the nature and seriousness of market misconduct, the SFC will have regard to the effects of the conduct on market integrity, the costs of the conduct caused to clients or the investing public, the duration and frequency of the conduct, whether there is a breach of fiduciary duty and whether any serious or systematic management or internal control failures are revealed. The SFC will also consider the degree of co-operation with the SFC and other authorities.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

There are no formal mechanisms in Hong Kong for the negotiated settlement of criminal investigations or proceedings that are equivalent to DPAs in the United Kingdom or the United States. However, in some limited circumstances, negotiations with, or representations made to, the SFC and the DOJ may result in a decision being taken not to prosecute.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Not applicable.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

The SFC has wide powers to enter into settlement agreements under the SFO, and may do so if this is in the public interest. In considering settlement, aside from considering factors such as the strength of the prosecution and defence cases, the costs and reputational damage of a lengthy investigation and potential subsequent legal proceedings, and possible penalties, institutions should also be aware that the SFC may insist on a public reprimand of the financial institution via an announcement on the SFC's website. The SFC will take into account the degree of co-operation in considering the settlement package.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Not applicable.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

The SFO gives a person who has suffered pecuniary loss as a result of market misconduct the right to bring a civil action to seek compensation. Compensation will only be payable if it is fair, just and reasonable in the circumstances of the case. Findings of the MMT in relation to market misconduct will be admissible as prima facie evidence in the private action, though proceedings before the tribunal are not a prerequisite for bringing civil proceedings. The SFC will not intervene in private legal proceedings.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

In practice, law enforcement agencies do not normally publish the commencement of investigations of criminal cases (although they sometimes announce high-profile arrests or dawn raids). Publicity usually follows when a decision has been made to charge an individual or during criminal proceedings once instituted. Criminal trials in Hong Kong are conducted in open court. Some agencies, such as the SFC or the ICAC, publicise the outcome of enforcement proceedings they have initiated on their websites from time to time.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

There are no particular factors specific to Hong Kong in managing corporate communications in Hong Kong. The steps are likely to be similar to those that would be taken to manage corporate communications in other jurisdictions, for example, timely, accurate and effective messages using the right media channels, while being sensitive and perceptive to the geopolitical environment. Public relations and media companies can be and have been used in Hong Kong to manage certain corporate crises.

72 How is publicity managed when there are ongoing related proceedings?

Publicity is usually managed by a press officer or communications department that will monitor media reports and suggest the making of public statements as and when necessary. Any public statements made by the company should be carefully drafted and any prejudicial effects on ongoing proceedings should be taken into consideration.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

For a listed corporation, settlement of a regulatory investigation may constitute inside information (depending on the nature and severity of the underlying offence or misconduct) and thus require disclosure as soon as reasonably practicable. In practice, the corporation and the authorities will usually agree on a press release being issued as part of the settlement and will agree on the timing for the release.

By way of context, inside information is defined to include specific information about the corporation that is not generally known to the public but would, if generally known, be likely to materially affect the price of the listed securities. Under Part XIVA of the SFO, a listed corporation must, as soon as is reasonably practicable after it becomes aware or is notified of any inside information, disclose the information to the public (subject to certain exceptions).

Anticipated developments

74 **Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?**

We do not expect the formalisation of DPAs in the next year or so in Hong Kong. Corporate misconduct, in particular, by listed companies, will remain a key enforcement priority of the SFC, the ICAC and the HKPF.

We also expect closer co-operation between the SFC and the CSRC in cross-border investigations, in particular concerning market manipulation in the context of the China-Hong Kong Stock Connect programme, and increased joint operations between enforcement agencies within Hong Kong, such as those mounted by the SFC and the ICAC into corporate misfeasance (see question 1).

17

India

Sherbir Panag, Tanya Ganguli and Lavanyaa Chopra[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The most high-profile corporate investigation currently under way is the Infrastructure Leasing and Financial Services (ILFS) case that is being investigated by the Serious Fraud Investigation Office (SFIO) and the Enforcement Directorate. The total outstanding debt of the ILFS is approximately 990 billion rupees. The issue came to light when, between July to September 2018, a few subsidiaries of the ILFS reported having problems paying back their loans and inter-corporate deposits (liquidity crunch). The government thereafter replaced the board of the ILFS and is presently investigating the allegations against the company.

Another issue that has grabbed the attention of the authorities is the role played by globally renowned auditing firms and credit rating agencies. The auditors, which include three of the four biggest auditing firms in India, failed to make adequate disclosures and point out red flags. They now face the risk of being banned for a few years. The credit rating agencies are being investigated for having given the ILFS the highest credit rating before downgrading the company when the investigations commenced.

2 Outline the legal framework for corporate liability in your country.

Corporations can be held criminally liable under the Indian Penal Code 1860 (IPC) since the definition of person includes any company or body of persons, whether incorporated or not. In 2005, the Indian Supreme Court held that corporations can be punished for offences,

1 Sherbir Panag is a partner and Tanya Ganguli and Lavanyaa Chopra are associates at Law Offices of Panag and Babu.

including those that require *mens rea* and also eradicated the immunity from prosecution demanding mandatory imprisonment, as provided to corporations.

In the 2018 amendment to the Prevention of Corruption Act 1988 (PCA), which is the premier anti-corruption legislation in India, a commercial organisation can be liable if an associated person (performing services for or on behalf of the commercial organisation) provides or promises to provide any undue advantage to a public servant to obtain or receive any unjustified gains. Further, under the Information Technology Act 2000 (the IT Act), a corporation can be held criminally liable for misuse of sensitive information.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Indian companies are governed by two sets of authorities – Enforcement Authorities and Regulatory Authorities. The Ministry of Corporate Affairs (MCA) is primarily concerned with administration of the statutes, rules and regulations that regulate the functioning of the corporate sector.

The premier anti-corruption enforcement authority is the Central Bureau of Investigation (CBI). Other authorities empowered to investigate cases of bribery and corruption in India include:

- the Central Vigilance Commission, a statutory body that supervises investigation of corruption in government companies, departments and among public servants;
- the SFIO, established under the MCA to investigate the affairs of companies suspected of fraudulent activities based on orders from the central government; and
- the Enforcement Directorate, established under the Ministry of Finance to investigate and prosecute cases pertaining to economic offences under the Prevention of Money Laundering Act 2002 (PMLA) and the Foreign Exchange Management Act 1999.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

There are a number of regulatory authorities that have been empowered under specific laws to investigate and prosecute offenders in India. The powers bestowed on these regulatory authorities often overlap and hence, at times, those authorities may work in tandem for specific investigations. Various authorities can therefore commence an investigation with respect to the same matter under different legal grounds. The threshold of suspicion necessary to trigger an investigation varies from case to case.

Under the anti-corruption laws, both the bribe receiver and the bribe giver can be prosecuted. Another recent development in the anti-corruption regime in India is that property that has been purchased through the proceeds of crime can be attached by the enforcement authorities through measures provided under the PMLA, depending on the gravity and nature of the alleged offence.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

The company can challenge a notice in the appellate body of the authority from which the notice was received. When a notice is sent by the Enforcement Directorate, the company can challenge the notice before the adjudicating authority under the PCA.

The company, on receiving a summons notice from the enforcement authorities, can file a writ petition before the high court of the concerned state to challenge a notice and request the court to quash it.

However, the high court does not normally quash such a notice unless, in its opinion, grave prejudice will be or is being caused to the person to whom it has been issued.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

The PCA provides a company with the opportunity to report to law enforcement authorities that it has been compelled to provide an undue advantage to a public official within seven days of the date of providing such undue advantage. However, India does not make use of co-operative agreements in order to provide immunity or leniency to individuals who assist or co-operate with authorities in cases of corruption.

7 What are the top priorities for your country's law enforcement authorities?

The Indian government has been battling the menace of corruption in response to a number of corruption cases. In 2017, the government – with the objective of fighting black money, corruption and terror funding – implemented the demonetisation of all 500 rupee and 1,000 rupee banknotes.

Other legislative developments brought in by the government include the following:

- Benami Transactions (Prohibition) Amendment Act 2016 provides that competent authorities can attach and confiscate properties that are illegally held by one person on behalf of another person.
- The Fugitive Economic Offenders Act 2018 (the FEO Act) was introduced to govern laws pertaining to those who have allegedly committed an economic offence but have absconded to another country to obtain asylum and avoid criminal prosecution in India.
- A goods and services tax has been implemented in an effort to control the circulation of black money in the economy.
- Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act 2015 governs provisions regarding tax evasion, especially the concealment of foreign income and assets.

Additionally, the Indian government has been entering into bilateral agreements and treaties in pursuance of information-sharing with tax havens. The government has been endeavouring to make use of technology to prevent corruption by promoting cashless transactions and launching Government e-Marketplace (in an effort to make public procurement-related transactions more transparent), among other initiatives.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Cybersecurity is regulated and implemented by the IT Act and the rules notified thereunder. The Ministry of Communications and Information Technology (MCIT) is empowered under section 87 of the IT Act to formulate these rules. Under section 69B, central government may authorise any agency of the government to monitor and collect data generated, transmitted, received or stored in any computer source. In line with the same, the MCIT has notified the Information Technology (Security Procedure) Rules 2004, the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules 2009 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011, which lay down the practices to be followed and the standards to be adhered to regarding cybersecurity.

Other key powers include the following:

- confiscating computer systems or other devices that have been used to contravene the law;
- entering public places, and searching and arresting without a warrant, if the person is guilty or is reasonably suspected of committing a crime;
- search and seizure;
- requiring attendance of a witness; and
- issuing summons.

For cybersecurity-related failings, Chapter 9 of the IT Act deals with penalties, compensation and adjudication. Under section 43A, when any corporate body, possessing, dealing or handling any sensitive personal data in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures, and thereby causes wrongful loss or wrongful gain to any person, the corporate body shall be liable to pay damages by way of compensation to the person so affected.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The Code of Criminal Procedure 1973 (CrPC), the IT Act, the IPC and the Indian Evidence Act 1872 (IEA) regulate this sphere. Acts such as tampering with computer source documents, propagating or sending offensive messages via a communication service, dishonestly receiving stolen computer resources or communications, identity theft, etc. are listed as punishable offences under the IT Act. The IT Act also grants powers to issue directions for the interception, monitoring or decryption of any information through any computer resource, and to authorise the monitoring and collection of traffic data or information through any computer resource for the purposes of cybersecurity. It also ensures that the enforcement authorities have the power to investigate and lay down penalties for breaches, and prescribes guidelines for compensation payable in such cases.

The procedure for investigation, prosecution and the resulting proceedings are governed by the CrPC and concerns arising out of evidence collection and retention are governed by the IEA.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Criminal law can have extraterritorial effect as laid down by the IT Act, CrPC and sections 2 to 4 of the IPC. Every person (including a person not a citizen of India) shall be punished under the IPC for committing an offence in India. Any person liable for an offence under any Indian law who is to be tried for an offence committed outside India shall be dealt with according to the provisions of the IPC for that act in the same manner as if the act had been committed within India.

The provisions of the IPC apply to any offence committed by any:

- citizen of India in any place without and beyond India;
- person on any ship or aircraft registered in India, wherever it may be; and
- person in any place without and beyond India committing an offence targeting a computer resource located in India.

The word 'offence' includes every act committed outside India which, if committed within India, would be punishable under the IPC.

The IT Act also applies to any contravention or offence under the IT Act committed outside India, by any person, irrespective of nationality, or any contravention or offence committed outside India by any person, if the act or conduct involves a computer, computer system or computer network located in India.

To initiate or supplement criminal proceedings beyond the territorial jurisdiction of Indian criminal courts, section 105 sets down reciprocal arrangements regarding process. Further, Chapter VIIA of the CrPC discusses reciprocal arrangements for assistance in certain matters and procedures for the attachment and forfeiture of property.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Data privacy issues

The ease of accessing information depends on the strength of the document and information retention laws in the country from where information is to be obtained. This would predominantly depend on the laws governing data privacy and attorney–client privilege. India has signed mutual legal assistance treaties (MLATs) with 39 countries for sharing information and to obtain evidence from another country's jurisdiction. An alternative approach is to send a letter rogatory to a foreign court.

Legislative differences

It is important to ensure that an investigation does not result in violation of any laws overseas while accessing the required information. Moreover, it can be difficult to get assistance and co-operation from the local government for the process of collecting evidence. Differences in laws on data protection, attorney–client privilege and labour laws specifically pose difficulties in proceeding with an investigation.

Extradition of the accused

The government has been grappling with the issue of economic offenders in high-profile cases fleeing abroad. The process of extradition from another country can lead to delays in investigations.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The concept of double jeopardy is enshrined in Article 20 of the Constitution of India. The doctrine of double jeopardy protects a person from being tried and punished twice for the same offence but not from different offences arising out of the violation of different laws by the same set of facts. However, a corporation facing criminal exposure in India after it resolves charges on the same core set of facts in another country may not avail itself of protection against double jeopardy.

While the judiciary has attempted to prevent multiplicity of case, multiple agencies with similar powers under the PCA, PMLA and Companies Act 2013 (the CA Act) are competent to investigate different aspects of similar sets of facts.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not the norm in India. However, global co-operation is practised with jurisdictions outside India. India has co-operated with other enforcement agencies such as the US Department of Justice (DOJ) and Securities and Exchange Commission (SEC), especially under the regime of the US Foreign Corrupt Practises Act (FCPA). Examples of global co-operation include the *Louis Berger* case and the recent *Cognizant/Larsen* and *Toubro* FCPA investigation.

Given the amendment to the PCA (see question 2), global settlements may commence in the year to come and subsequently become fairly common in India.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

It is a settled principle that decisions in criminal cases by courts in foreign countries cannot be enforced in India. It was recently held by the Bombay High Court in *Prabodh K Mehta v. Charuben K Mehta* (2018) 3 Bom CR 1 (Bom)(FB), that the conviction of an individual in a foreign court will not be *ipso facto* binding on Indian authorities.

However, the conviction will not be overlooked and will be recognised under the principle of comity. Indian authorities may seek relevant information from the foreign courts for the purpose of proceeding with an investigation in India. While the conviction will not be completely relied upon, the information that is available by way of the decision of the foreign courts may form a source of evidence while proceeding with an investigation in India.

It is also important to note that the stance of the Indian judiciary varies in civil matters. Under sections 13 and 14 of the Civil Procedure Code 1908 (CPC), foreign judgments are automatically enforceable in India, unless there is proof in support of the contrary and it is contested by the parties.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Sanctions against a corporation can be in the form of a fine or imprisonment of key personnel associated with the commercial organisation involved in the wrongdoing or misconduct, or both. Penalties imposed on corporations can also take the form of fines.

In 2018, SEBI banned a big four auditing firm, PricewaterhouseCoopers Private Limited (PwC), from auditing listed companies in the country for two years following PwC's failure to detect fraud of more than US$1 billion at the IT services company, Satyam Computer Services, which is one of India's largest corporate fraud matters to date.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

India has witnessed a rise in the economic sanctions being imposed on corporations and the key personnel in such corporations. There has also been an evident increase in the number of dawn raids carried out by government authorities in connection with matters involving corruption and tax evasion.

On account of an increasing number of delinquent borrowers and non-performing assets, law enforcement authorities have shifted their focus towards fraud and evergreening of loans in the financial sector. In the recent *Punjab National Bank* fraud case, the Enforcement Directorate has taken a stringent stance on prosecuting the perpetrators, including the fugitive, Mr Mehul Choksi.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Enforcement authorities co-operate for the purpose of sharing information relevant to their respective investigations. Both formal and informal mechanisms can be used to coordinate with each other. Formal mechanisms include the following:

- MLATs: These can be multilateral or bilateral agreements for gathering and exchanging information in furtherance of enforcing public and criminal laws. India has such treaties with 39 countries.
- Extradition treaties: These lay down the framework for one state to surrender an individual to another state for prosecution or punishment of crimes committed in the requesting country's jurisdiction. India has signed bilateral treaties with 43 countries.
- Extradition arrangements: These are arrangements wherein detainment of the accused would depend on the local laws of that country and international regulations. India has extradition arrangements with 10 countries.

- Tax information exchange agreements: These provide for the exchange of information in a request relating to a specific criminal or civil tax investigation or civil tax matters under investigation. India has such agreements with 17 countries.

Informal mechanisms include co-operation between the intelligence and diplomatic services of various countries for the exchange of information.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

The Indian Parliament has not promulgated any blocking legislation. However, the government has the option of imposing countermeasures that prevent Indian entities from avoiding compliance with extraterritorial sanction measures. To conclude, there is no policy or mechanism currently favouring Indian companies.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

India has not enacted sanctions blocking legislation. However, if countermeasures are enacted, companies could find themselves caught between the conflicting directives of the sanctioning country and the country seeking to implement countermeasures.

In June 2019, India introduced retaliatory tariffs on certain goods imported from the United States in response to the higher tariffs imposed on steel and aluminium imports by the Trump administration.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct most often come to light by way of the following means:
- whistleblower complaints;
- red flags highlighted as part of due diligence conducted during acquisitions and takeovers;
- competitors and industry sweeps;
- traditional police investigations;
- suspicious activity reports;
- audits and compliance checks; and
- media investigations and reporting.

However, the Whistle Blowers Protection Act 2011, which is yet to come into force, does not apply to corporate whistleblowers. The Act covers only those who make disclosures of wrongful acts committed or attempted by a public servant. Nonetheless, whistleblowers are usually protected under their respective company's whistleblower policy. The SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015 require listed companies to devise an effective whistleblowing policy.

Information gathering

21 Does your country have a data protection regime?

India presently does not have any express legislation governing data protection or privacy. The key legislation in this sphere is the IT Act. Additionally, the transfer of personal data is currently governed by the Sensitive Personal Data and Information Rules 2011 (the SPD Rules).

The IT Act deals with payment of fines and imprisonment under civil and criminal laws for cases of wrongful disclosure and misuse of personal data, and violation of contractual terms regarding personal data. The Personal Data Protection Bill 2018 focuses on consent being central to data sharing, with respect to data processed by both government and private entities. However, in *Justice Puttaswamy (Retd) v. Union of India* (2017) 10 SCC 1, also known as the *Aadhar* judgment, the Supreme Court of India, while establishing the right to privacy as a fundamental right, held that it was not an absolute right and could be made conditional on reasonable grounds.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The IT Act, through the Finance Bill, merged the Cyber Appellate Tribunal with the Telecom Disputes Settlements and Appellate Tribunal, which are the two adjudicatory bodies for infringements of the IT Act. When compensation for failure to protect the confidentiality of sensitive information is less than 5 million rupees, the IT Act provides for the government to appoint an adjudicatory officer with the powers of a civil court. However, although there are penalising provisions, the enforcement of the provisions is not widespread.

Section 50 of Data Protection Bill contemplates the establishment and incorporation of a data protection authority by central government. This authority will consist of six full-time members appointed for a five-year term by central government.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

Companies are required to incorporate policies and practices that impose stringent measures concerning document collection and internal investigations. Under the IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, a company can be penalised for negligence in handling sensitive personal information. Further, recipients of sensitive personal data or information may be obliged under attorney–client privilege laws to exercise extreme caution while handling data during investigations.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

The IPC criminalises the disclosure or destruction of any document or electronic record that may be required to be produced as evidence in legal proceedings. During an investigation, it is general practice to circulate a document hold memorandum to those employees who are suspected of having documents relevant to the investigation, in an effort to preserve the

documents. This would also be likely to include access to electronic data for further analysis, such as email forensics.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants are governed by section 93 of the Code of Criminal Procedure, 1973, which establishes certain stipulations regarding the issuing of search warrants:

- They can be issued only by a magistrate.
- The magistrate must apply his or her judicial mind while issuing a search warrant.
- There must be a search and seizure report (known as a *panchnama*) following any search or seizure.

Chapter XIV of the CA Act makes provisions pertaining to inspection, enquiry and investigation in corporate entities. Central government has established the SFIO under section 211 of the CA Act to investigate fraud relating to a company. The provisions of the CPC apply, *mutadis mutandis*, to every search and seizure made under these provisions.

Further, section 41 of the Competition Act 2003 empowers the director general of the Competition Commission of India to conduct dawn raids. The director general is required to obtain a warrant from a magistrate before conducting a raid after satisfying the competent court with material documents and evidence of anticompetitive conduct.

The Companies (Arrests in Connection with Investigation by Serious Fraud Investigation Office Rules 2017 were notified by central government on 24 August 2017. Under the notification, the SFIO is required to follow a number of procedures before making an arrest. These act as a limitation and further delay the SFIO's initiatives to arrest an accused. For instance, the arrest of an individual in connection with a government company or a foreign company under investigation must be made with prior written approval from central government. Further, the initiation of this arrest must also be given to the managing director or other person in charge of the affairs of the company.

Furthermore, a seizure report must be issued. A seizure report is the official record of a raid. It documents the operation and must be prepared by the law enforcement authorities conducting the raid. Among other things, the seizure report must specify the material particulars pertaining to the raid, such as the address of the site being raided, particulars of the person occupying the site at the time of the raid, particulars of the investigating officer or officers, and details of any independent witnesses present. Most importantly, the seizure report must contain a detailed statement of all the materials, documents, objects or articles seized from the site. The completed report must be vetted by two independent witnesses who observed the raid. The investigators usually request company representatives to sign the seizure report and can provide a copy of it upon request.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

The company may object to the review or taking of copies of privileged documents during a dawn raid, including confidential communications between the client and its external attorney. Sections 126 to 131 of the IEA govern attorney–client privilege in India. However, attorney–client documents are not protected in the strictest sense from the police or other law enforcement agencies, should they be found during a dawn raid or a search under a valid warrant. It would depend on the law enforcement agency's discretion whether to respect the company's request not to access such documents. If the authorities decide that the documents are not privileged or confidential, company counsel should request that the documents be placed in sealed envelopes when seized. The objection to the taking of such documents shall also be documented or recorded.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Principally, an individual's testimony cannot be compelled in India for acts of bribery or fraud. The Constitution under Article 20(3) states that no person accused of any offence shall be compelled to be a witness against himself or herself. Further, under section 161 of the CrPC, individuals being interviewed by the police are not bound to answer questions that could expose them to a criminal charge or to a penalty. Compelled testimonies constitute an infringement of an individual's rights and freedom.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The PCA itself does not provide any protection to whistleblowers. A separate act – the Whistleblower Protection Act 2011 – is primarily intended to protect whistleblowers with respect to disclosure of:

- acts of corruption by a public servant;
- wilful misuse of power by a public servant; and
- wilful misuse of discretion or the commission, or attempted commission, of a criminal offence by a public servant.

The Whistleblower Protection Act has been passed by both houses of Parliament but has not yet been brought into effect by the government by way of a notification in the Official Gazette. There are no provisions for providing financial incentives for whistleblowers. Moreover, the Act does not deal with corporate whistleblowers, and therefore does not extend its jurisdiction to the private sector.

The SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015 require listed companies to devise an effective whistleblowing policy. Further, the Central Vigilance

Commission can initiate investigations based on allegations or complaints by employees of a government corporation.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employees are governed by both central and state legislations. However, these laws do not specifically elaborate on employee rights with respect to investigations. Employees are required by their contract or internal policy of the employer to co-operate in an internal investigation. In appropriate cases, non-participation may entitle the employer to take disciplinary steps against an employee. However, the employer has no coercive powers, and all individuals have a right against self-incrimination under Indian laws.

No special protection is provided to key managerial persons in the event of internal or external investigations under labour laws. The only difference lies in the fact that the circumstance leading to the dismissal of a director who has been appointed by the board, is provided under the CA Act.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

The rights of an employee deemed to have engaged in misconduct depend on the employment contract and the compensation policy of the company. These may include various retaliatory actions, such as denial of pay rises, suspension or termination of employment or warnings.

A number of Indian companies have resorted to clawbacks of bonuses or stocks from key managerial persons who have been involved in misconduct and acted against the interests of the company shareholders. In May 2019, Yes Bank – one of the leading private sector banks in India – announced that it would be clawing back bonuses amounting to approximately 20 million rupees from a former managing director.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

If a company has adequate proof of misconduct against an employee who refuses to participate in an internal investigation, the company may dismiss the employee, while adhering to the principles of natural justice. However, the process shall be governed by the employment contract and relevant policies of each company.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Structuring the scheme of an investigation will follow a preliminary analysis of the allegation framework and the documents available that pertain to it. Thereafter, the investigators shall draw up broad terms for conducting an investigation, which will entail the following:

- deciding who has to be investigated – the informant, reporter or whistleblower, the accused, witnesses and other relevant individuals;
- the objective and scope of the investigation;
- the legal issues under consideration;
- a potential defence strategy, if any;
- materials in the form of documents, business structures, emails, official call records, etc., required for substantiating the allegation that initiated the investigation; and
- setting a deadline for concluding the investigation and submitting the findings of the investigation.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

If an issue comes to light prior to the authorities becoming aware or engaged, the company shall first and foremost conduct an internal investigation and seek legal advice on how to proceed with the issue. Subsequently, on conclusion of the internal investigation, the company shall, based on the findings of the investigation, implement countermeasures or adopt policies to prevent similar issues in the future.

The company shall generally have an effective whistleblower policy, which shall ensure that the identity of the whistleblower is kept confidential. Companies listed in the stock exchange are required to have an effective whistleblower policy in place. Further, depending on the applicable laws, it may be mandatory for a company to make disclosures to law enforcement agencies.

However, there are no legal or statutory requirements for a company to take any internal steps on becoming aware of any issue, except in the case of a complaint alleging sexual harassment in the workplace. The Sexual Harassment of Women (Prevention, Protection and Redressal) Act 2013 requires every branch or office or company employing 10 or more persons to constitute an internal complaints committee.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

A company that is the subject of an external investigation must co-operate fully and furnish complete and correct information and documents within the time provided by the law enforcement agency.

If the law enforcement agency has sought the production or preservation of documents or data, the company should impose a document hold to ensure the preservation of certain documents and information that may be necessary for completion of the inquiry, or in anticipation of any future litigation. Further, the appointment of a document custodian to maintain control over the relevant documents and information would be advisable.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Disclosure of the existence of an internal investigation or contacting a law enforcement authority will depend on the nature and gravity of the case. Under section 39 of the CrPC, an individual can be penalised for not reporting the commission of a crime by another entity, or the intention to do so. However, in other circumstances, the counsel or advocate of the entity will advise with respect to the disclosure of an investigation or contacting an authority. In India, there is hardly any incentive to approach law enforcement agencies, since it does not provide for any guarantee of immunity or leniency.

36 How are internal investigations viewed by local enforcement bodies in your country?

Investigations allow corporate entities to flag problem areas. The past few years have been significant as regards the development of white-collar criminal jurisprudence in India. Owing to greater pressure for compliance, an increasing number of organisations now opt to conduct internal investigations. Internal investigations aid in keeping a check on the affairs of the corporate entity and protect against unwarranted raids, and any other actions by authorities.

Moreover, before approaching a law enforcement agency, it is advisable that companies carry out their own investigation to substantiate the claims themselves. Commercial organisations can thereby analyse whether the procedures in place were adequate to prevent wrongdoings and subsequently claim it as a defence. This also aids in highlighting the company's strong stance against such misconduct, and may prevent an adverse action by the law enforcement authorities against them.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Legal advice given by a lawyer to a client is privileged under the IEA, the Advocates Act 1961 and the Bar Council of India Rules. As a rule, attorney–client privilege is subject to certain exceptions (e.g., communications made in furtherance of illegal purposes or offences discovered in the course of advising a client are not privileged.).

In *Larsen & Toubro Limited v. Prime Displays (P) Ltd* (2003) 114 CompCas 141 (Bom), it was held that a document that has come into existence in anticipation of litigation will be covered by privilege. The documents should have come into existence while seeking legal advice or for use for the purpose of defence or prosecution of the legal proceedings. Legal

advice is not confined to telling a client the law; it must include advice as to what actions or steps shall be undertaken in a certain set of circumstances.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

The IEA governs the law regarding privileged communication that is attached to professional communications between a legal adviser or counsel and a client. No one shall be compelled to disclose to a court any confidential communication between an individual and his or her legal adviser or counsel, except when offering himself or herself as a witness, to the extent necessary for providing evidence.

The key elements for ensuring privilege in correspondence are:

- to provide sound legal advice and advocacy;
- to maintain the client's privacy;
- that parties should have agreed upon the representation of the client;
- that the client can waive privilege; and
- to protect client communications, including the slightest action or inaction.

The client is the holder of the privilege. When the client is a corporation, the privilege is part of corporate control whereby the officers and directors decide whether to assert or waive the privilege. However, principally there is no difference in the privilege when the client is an individual or a corporation.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Attorney–client privilege does not apply equally to in-house and external counsel. External counsel with the required expertise are often engaged to conduct internal investigations.

Documents created in the course of an internal investigation, or as an outcome of an investigation, are generally protected. The extent of privilege available to communications with in-house counsel would be limited. The privilege would extend only to the legal advice and work undertaken by the in-house counsel in lieu of litigation. It shall not cover any work of an executive nature undertaken by the in-house counsel.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Foreign lawyers are prohibited from practising in India. Under the English law of privilege, communications between clients and their foreign lawyers will be protected on the basis of the law of the land where protection is sought. In India, the position is unclear, although 'barristers' (i.e., barristers 'of England or Ireland, or a member of the Faculty of Advocates in Scotland', as defined under the General Clauses Act 1897) are bound by attorney–client privilege.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Section 126 of the IEA provides certain exceptional grounds on which attorney–client privilege shall stand denied. This includes communications with an attorney regarding furtherance of any illegal purpose or becoming aware of facts that either a crime or fraud has been committed since the commencement of the attorney's employment. The client's intention to reveal such information to the attorney is irrelevant.

Under section 128 of the IEA, the privilege will be considered to be waived if the client calls his or her attorney or legal adviser as a witness and questions him or her on the same. In *Mandesan v. State of Kerala* 1995 Cri LJ 61, it was remarked by the sitting judge that there shall be express consent either by the client or the attorney to waive privilege.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Sections 126 to 129 of the IEA do not contemplate limited waiver and a client may waive privilege entirely or not at all. The same shall be expressly consented to by either of the parties. Further, the Act does not contemplate sharing of attorney–client communications or work-product with a third party with common intentions without waiving protections.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Privilege that has been waived on a limited basis in another country will be maintainable in India only if the same is proven in India. Indian courts will assess the laws of the country under which the privilege has been waived on a limited basis.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Sections 126 to 129 of the IEA do not contemplate sharing of attorney–client communications or work-product between persons with a common interest without waiving protection. The scope of attorney–client privilege extends only to the persons and circumstances mentioned under sections 126 to 129 of the IEA.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Communications between an attorney and a client are privileged even if they contain information from third parties. This privilege also extends to interpreters, clerks or servants of the attorney. Information sought or requested by the client and provided by an employee or third party for legal advice or litigation is also protected. However, communication between the employees of the client in the ordinary course of business, not in anticipation of litigation, is not protected. Accordingly, there is no protection accorded to:

- statements made by an employee on or relating to the subject matter of the proceedings that were not requested to be provided to the attorney; or

- written communications from one employee to another that is potentially useful to the attorney.

To claim privilege, the communications should be of a private and confidential nature, and must have been provided in confidence. Communications made in the presence of third parties would be privileged if it were proven that it was the intention of the client.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

It is common practice to carry out interviews of witnesses during internal investigations. There are no set statutory rules for conducting a witness interview involving an employee in India, and the purpose of the interview usually depends on the requirements or procedures to be followed in the investigation. Based on the preliminary documentary review pertaining to an investigation, there may be a need to proceed with interviews of a certain set of sampled individuals.

Authorities are not required to be consulted before initiating witness interviews. However, in most cases, the witnesses shall be informed about the interview beforehand.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Companies and corporations enjoy a right to privilege with respect to information disclosed or documents provided to external legal counsel for the purposes of an internal investigation. Internal witness interviews and attorney reports constitute legal advice and therefore fall under the ambit of attorney–client privilege.

However, in practice, in-house counsel are required to sign employment contracts with confidentiality clauses, whereby damages can be claimed from in-house counsel in the event of a breach of a confidentiality clause.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Upjohn warnings are issued before commencing an interview. Additionally, investigations are to be conducted in accordance with principles of natural justice. Generally, documentation of an investigation relates to interviewing the complainant, alleged accused and other relevant witnesses. Two of the key principles to keep in mind while conducting witness interviews are as follows:

- proper representation to the interviewee that the attorney–client privilege extends, belongs solely to and is controlled by the company or corporation that has engaged the counsel to conduct the investigation; and
- the corporation may decide to waive the aforementioned privilege and disclose the information provided by the interviewee to any government or enforcement agency, or any third party.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

It is imperative to assess the logistics of conducting an interview. Most investigations endeavour to elicit complete information at the first opportunity during the initial interviews. Interviews help investigators to understand the motives and truthfulness of the person being interviewed.

Planning for interviews includes a number of processes that are determined in each case. However, the following factors must always be looked into:

- deciding or sampling the interviewees;
- fixing the venue and scheduling time slots for conducting the interviews;
- investigating the witnesses' background;
- deciding the sequence of conducting interviews, especially when a significant number of individuals are required to be interviewed. Moreover, this step shall include anticipating witness questions and preparing an outline for each of the witness interviews; and
- documenting and recording the findings of the interviews.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

There is no legislation mandating the reporting of misconduct in India. Most companies prefer to conduct an internal investigation to substantiate the allegation themselves before proceeding to inform the law enforcement authorities. Disclosures made by companies have to be voluntary. A disclosure will be viewed as the company co-operating with law enforcement and may contribute towards acquiring a favourable judgment in court. However, listed companies must check their disclosure obligations in accordance with the listing agreement signed with the stock exchange.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

The self-reporting mechanism in India is at a nascent stage. Statutes providing leniency in return for disclosures are scarce in India and are limited to the Competition Act 2002 and the Income Tax Act 1961. Self-reporting to the concerned authorities in cases of serious fraud, corruption or criminal acts have to be voluntary. Self-reporting may be advisable when followed by a robust internal investigation undertaken by the corporation itself. However, under the Prevention of Corruption (Amendment) Act 2018, a company that has been compelled to pay bribes may be exempted from liability, on reporting it to the relevant law enforcement authority within seven days of the date of making the illegal payment.

Advice to self-report in other countries would depend on the laws in that country. For example, in the United States, there are mandatory self-reporting clauses under various pieces of legislation. Additionally, the DOJ and SEC consider self-reporting as a mitigating factor for providing leniency in cases of bribery, corruption and fraud.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

Before approaching the law enforcement authorities, it is imperative to first substantiate the allegations internally. Therefore, an internal investigation must be carried out wherein the purpose of the investigation is clearly defined, and an internal report is prepared that sets out the findings of the investigation.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

The company would first want to ensure that the communication received is in fact a notice from a law enforcement agency. The company shall contact its counsel, note the scope of the search by the authorities and keep a record of any items that are seized during the procedure. Notices may be issued under various circumstances and legal assistance may be sought to determine the nature of the legal communication received.

The following must be analysed in such a circumstance:

- full name of the issuing court, tribunal or authority in the document's title or letterhead;
- the parties addressed or the company's name, or both;
- a specific date, time and location for appearance or the materials demanded;
- in certain cases, the penalty for non-compliance;
- the document title; and
- the provision under which the notice has been issued, the liability or the charges alleged.

Whether the company can address these issues before the charges are brought varies from case to case. When a notice is issued to a company during the course of a criminal investigation by the police department or enforcement agency, it could be possible to discuss the issues with the investigating officer to aid investigation. However, this option is not available in every situation.

If the notice has been issued by a court or tribunal, then the company must enter proceedings before the tribunal and no dialogue may be possible after charges are brought. In such cases, the company must send an appropriate representative to court.

54 Are ongoing authority investigations subject to challenge before the courts?

If investigations are initiated, a petition for quashing the first information report (a written document prepared by the police when they receive information about the commission of a cognisable offence) may be filed before the high court of the concerned state. However, if the National Company Law Tribunal is taking cognisance of the matter, there cannot be a challenge to an ongoing investigation.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

If different notices have been issued by different law enforcement agencies, they would have to be responded to separately. This is because different violations or offences could arise from the same set of facts. These violations or offences could be subject to the jurisdiction of different law enforcement agencies and each of these agencies must be provided with an explanation.

The company may request the courts to admit information or decisions of a foreign court along the same set of facts. However, such a request is merely persuasive and not binding. Additionally, judgments or orders of local courts arising out of the same set of facts may also be presented.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

While an Indian company is not obliged to procure and produce evidence from a foreign counterpart, the concerned enforcement agency may request such evidence through the relevant tribunal or court. While there are formal means (through bilateral treaties) of seeking the production of information from other jurisdictions, these can have their limitations in terms of delays, ambiguities and incomplete information.

Further, letters rogatory, also known as letters of request, are formal requests from a court in a foreign jurisdiction for judicial assistance, especially to begin the process of examining the relevant individual as a witness or gathering relevant evidence. In 2017, the Ministry of Home Affairs also issued a Comprehensive Guideline for Investigations Aboard and Issuance of Letters Rogatory in 2007. The Indian government has resorted to letters rogatory with respect to high-profile corruption matters. The Enforcement Directorate had issued letters rogatory to the United Kingdom in the loan fraud cases against the liquor baron, Vijay Mallya.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Both the law enforcement agencies and the court systems can share information and investigative materials with foreign countries. For legal co-operation in civil and commercial matters, MLATs are signed with the countries concerned. These assist in seeking co-operation for judicial proceedings, collection of evidence, investigation and witness examination.

For sharing information and investigative materials for criminal matters, the court or tribunal may issue letters rogatory to the court within whose jurisdiction the accused or witness resides, or the evidence may have been found.

Furthermore, India has guidelines for its law enforcement on extradition proceedings against fugitives, especially economic offenders under the FEO Act.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Disclosure obligations primarily depend on the nature of the document and the legal status of the company. Courts normally do not promote disclosure of sensitive information revealed during the investigation. However, there is no specific legislation imposing confidentiality obligations on law enforcement. Discovery statements (statements made to the police that can be proved by subsequent discovery of facts) under section 27 of the IEA can be further used as evidence by the judiciary for furtherance of a case.

Under the SEBI (Listing and Disclosure) Regulations 2015, companies are required to make disclosures pertaining to their compliance of mandatory requirements and adoption of the non-mandatory requirements. Further, refusal to produce information or documents may be viewed as a sign of non-co-operation, which can eventually result in the law enforcement making adverse findings.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

There is no specific legislation providing for an Indian law enforcement agency to request a company in India to provide documents from another country. As counsel, we would normally advise the client to refrain and to reject such a request. However, the advice may be altered or modified on the basis of other compelling aspects, such as the gravity of the offence and the charges levied.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Although India has statutes that provide for the protection of data, there is no blocking statute. The aim of these data protection laws is to ensure that sensitive personal data is not leaked without the permission of the data provider.

These protections do not apply when a statutory or judicial authority seeks information; therefore companies must comply with the requests made by the appropriate authority. Under the IT Act, authorities may access computer systems or other devices to collect information that may constitute evidence for a court proceeding or government investigation.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Confidentiality for voluntarily produced documents cannot be ensured. The material so reproduced before law enforcement agencies could be reproduced to the court. Therefore, it is at the discretion of the courts if the information or material produced should form part of the judgment.

Under section 91 of the IPC, a court can compel the production of any document. However, under section 129 of the IEA, no one can be compelled to disclose confidential information protected by attorney–client privilege; a client would need to waive privilege before protected information is disclosed. If the client does waive privilege, his or her attorney can be compelled by the court to provide as evidence any communication or document previously protected.

Further, an international agency (for example, Interpol or a foreign government) that seeks the assistance of the Indian law enforcement agencies in gathering information with respect to an investigation, a witness or evidence may be provided with the confidential information.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Company officials or employees may be penalised with imprisonment, fines, debarment or disgorgement, or a combination of any of these sanctions, depending upon the nature and gravity of the offence and the governing provision. For example, under section 24 of the SEBI Act 1992, a person found guilty may be imprisoned and fined 250 million rupees, or three times the amount of profit made, whichever is higher.

In many cases, often the assets of the accused individuals are also attached until the investigation is completed.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

In most cases, the suspension, debarment or other restrictions on a corporation in India will not result in automatic suspension or debarment in another country. Restrictions or options applying to a company in another country will depend on the nature and magnitude of the offence and whether that offence is listed as a criterion for suspension in another country.

Legislation in other countries with extrajudicial reach may have an effect on the corporation's options in India and that country. However, that would entail only after investigations regarding the claim are carried out in that country.

64 What do the authorities in your country take into account when fixing penalties?

To determine liability in any offence, the two elements to be established are (1) the commission of the punishable act and (2) the intention to commit that act.

Individuals at lower levels of management or the workforce often do not participate in the decision-making process in a company and since the corporate entity cannot develop an intention on its own, directors and top management are therefore regarded as the 'directing mind' of the corporate entity. These aspects are scrutinised while ascertaining and accruing the liability of an entity. Other factors such as the nature of the offence, its effects and gravity, parallel provisions, the threshold of compliance, etc. are also taken into account. Further, co-operation and good conduct on behalf of the company towards the law enforcement authorities can contribute towards the courts imposing more lenient penalties on the accused.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Neither non-prosecution agreements nor deferred prosecution agreements are available in India for corporations. These terms are not recognised under any of the Indian statutes. However, the Competition Commission of India has the power to impose lesser penalties under the Competition Act 2002 if it is satisfied that any producer, seller, distributor, trader or service provider included in any cartel, which is alleged to have entered into an anti-competitive agreement, has made a full and true disclosure in respect of the alleged violations. If that disclosure is vital, the Commission has the power to impose upon the producer, seller, distributor, trader or service provider a lesser penalty, as it may deem fit, than is provided for under this Act or the rules or the regulations. Depending upon how useful or at what stage such a disclosure is made, the penalties may be reduced.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

These provisions do not exist under the Indian legal system.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Offences of fraud, corruption and bribery are non-compoundable under the Indian criminal law and the PCA does not have a provision in support of plea bargaining.

Additionally, when a case concludes in favour of a company, then the application of double jeopardy will prevail, wherein the accused company or entity cannot be tried again on the same or similar charges and on the same facts, following an acquittal or conviction.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Private entities are prohibited from being involved in investigations under the CA Act unless they are the ones being investigated or required by statutory or legal authority to make disclosures. Further, while India does not impose corporate monitors on companies involved in bribery and fraud, the SEC does impose corporate monitors on companies that may have operations in India. The SEC has previously imposed corporate monitors on Walmart for two years to guard against corruption in its foreign ventures.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

In India, parallel private investigations can be conducted by companies in addition to government investigations. Internal investigations by companies allow for an understanding and the detection of the root cause of the crisis. Findings of such investigations can subsequently be

shared with law enforcement agencies and form part of the evidence. Although this mechanism is not part of any present legislation, such a step by a company may be considered by the court and result in leniency in penalties. Additionally, under The Right to Information Act 2005, a person can request access to any government record or document unless it is confidential.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

There are no specific laws or policy guidelines regarding publicity of cases relating to white-collar crimes at the investigatory stage. However, in 2016, the Supreme Court of India held that a 'first information report' is a public document and, therefore, the media may publish information pertaining to such cases at any stage (including the investigation stage). The press in India is free to attend legal proceedings and report ongoing matters. Generally, the Indian media report on investigations as soon they commence, especially in high-profile cases.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Companies may either have an in-house public relations department, with communications and publicity managers, or may outsource the services to another entity specialising in handling publicity-related tasks. Companies also consult their legal and compliance teams before disclosing any such information to the public.

72 How is publicity managed when there are ongoing related proceedings?

Since all investigations are not made public, companies under normal circumstances attempt to ensure that no public disclosure is made at all. If investigations or proceedings become public, public relations agencies are engaged to manage the media. Consultants who have experience in handling government relations during a crisis are also engaged for damage control. Companies may also, at times, provide public disclosures on their official website, if they are directed to do so during the investigation procedure.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Normally, information pertaining to a settlement would be disclosed soon after a settlement has been agreed. However, plea bargaining or similar settlement mechanisms are not prevalent in India in matters pertaining to fraud and corruption, which are considered as serious crimes.

Anticipated developments

74 **Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?**

India has witnessed a rise in corporate misconduct in the banking sector recently, especially in relation to non-banking financial companies. There have also been numerous incidents of high-profile corporate misconduct within well-known audit companies. The government is expected to create regulations governing specific sectors that have been at the forefront of this corporate misconduct.

Further, the Whistle Blowers Protection (Amendment) Bill 2015, which has not yet been enforced in India, provides for a mechanism for receiving and enquiring into public interest disclosures against various acts of corruption, wilful misuse of power or discretion, or criminal offences by public servants.

18

Ireland

Claire McLoughlin, Karen Reynolds and Ciara Dunny[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The investigation into the Irish Bank Resolution Corporation by a Commission of Investigation remains the highest-profile ongoing corporate investigation in Ireland. It is very significant as it is connected to the collapse and subsequent wind-down of Anglo Irish Bank plc, a prominent Irish bank that collapsed in connection with the financial crash. The related trial of certain high-ranking banking executives concerning their conduct before the collapse was the longest criminal trial in the history of the state and resulted in penal sentences, which are rarely imposed in Irish business crime cases. This investigation is one of the most complex ever to have been carried out by the Garda National Economic Crime Bureau (GNECB) and concerns allegations of a €7.2 billion conspiracy to defraud.

It is important for both the subject matter under investigation and the procedural conduct of any similar investigation in the future. In that regard, the Commission of Investigation has published a number of interim reports that have highlighted difficulties in conducting this type of investigation in Ireland, such as duties of confidentiality, privilege and the constitutional rights of persons implicated in the investigation.

A draft order and terms of reference for a Commission of Investigation into the National Asset Management Agency (NAMA) were published by the Irish government and an interim report was published in September 2017. The terms of reference provide for an investigation into Project Eagle (the name given to NAMA's Northern Ireland property loans portfolio), which it sold in April 2014 for about €1.6 billion. This was previously the subject of an inquiry in Northern Ireland.

1 Claire McLoughlin and Karen Reynolds are partners and Ciara Dunny is a senior associate at Matheson.

The Office of the Director of Corporate Enforcement (ODCE) has also recently launched high-profile investigations into both Independent News & Media PLC (INM) and the Football Association of Ireland (FAI). In September 2018, the president of the High Court granted an application by the ODCE to appoint inspectors to INM and investigate whether there may have been alleged unlawful sharing of the company's information. The investigation into the FAI was commenced subsequent to its auditors filing a notice to the Companies Registration Office alleging breaches of the Companies Acts on the grounds that financial accounts were not properly maintained. If it is proved that there was a failure to keep proper accounting records, this would result in a breach of sections 281 to 285 of the Companies Act, and the potential conviction of individual board member, who could face a fine of up to €50,000 or imprisonment for up to five years, or both.

There has been only a very limited number of applications to appoint inspectors by the High Court. The approach in relation to the INM investigation was the first brought under section 748 of the Companies Act 2014, which is a relatively new provision but one that is very similar to the legislation under which previous applications were made and which this provision has replaced. The judgment, therefore, provides guidance on the scope of the powers of the High Court. Significantly, the Court clarified that the actions of a director or chairman, even if acting outside his or her usual authority, will come within the meaning of conducting the 'affairs of the company' for the purposes of a section 748 application.

The High Court provided a useful analysis of the matters it will take into consideration in exercising its discretion under section 748, confirming that public interest in ensuring that proper standards of probity and good governance in companies are maintained is one of the primary matters that should be taken into account for any such application. The Court noted that public interest in the circumstances of this case was particularly engaged because of the nature of the company's business, the position it occupies in the Irish media sector and its status as a public company.

The Court also held that another important factor in the exercise of its discretion is the existence, or potential existence, of other statutory investigations into the subject matter of an application. Such investigations do not automatically preclude the appointment of inspectors and the Court will engage in an assessment of the adequacy of those investigations to deal with the issues raised in an application, taking into account matters such as the nature of the powers available to the statutory bodies in question, their power to publish a report and the effect and status of such reports.

An interesting side aspect of the judgment is that it brings renewed focus to an issue that has been occupying headlines for quite some time; specifically, the role of the ODCE and its ability to carry out its enforcement functions effectually. As a result of the Anglo Irish Bank investigation and recent trials, the ODCE has found itself subject to scrutiny as a result of comments made by Judge John Aylmer regarding its investigative process. Against that backdrop, the government, in its Package on White Collar Crime announced in November 2017, committed to re-establish the ODCE as a new independent agency in an effort to enhance the state's corporate law enforcement capacity. Under the General Scheme of the Companies (Corporate Enforcement Authority) Bill 2018, which was published in December 2018, it is proposed that the ODCE will be re-established in the form of a commission, known as the Corporate Enforcement Authority (CEA). The CEA will be established as an independent company law compliance and enforcement agency and will have greater powers than the

ODCE. The CEA will operate independently of any government department to provide more independence in addressing company law breaches. The establishment of the CEA is regarded as a fundamental element of the government's commitment to enhance Ireland's ability to combat white-collar crime.

During 2018, the government made some significant progress in implementing the proposals set out in the Measures to Enhance Ireland's Corporate, Economic and Regulatory Framework. This included the enactment of the Criminal Justice (Corruption Offences Act) 2018, which commenced on 30 July 2018, and publication of the General Scheme of the Companies (Corporate Enforcement Authority) Bill 2018 in December 2018. In addition, the Minister for Justice and Equality appointed Mr James Hamilton, former director of public prosecutions, to chair a review of Ireland's anti-corruption and anti-fraud structures and procedures in criminal law enforcement. In March 2019, the review group issued a call for submissions on a number of issues under its terms of reference, the results of which have yet to be published.

2 Outline the legal framework for corporate liability in your country.

Corporations are separate legal entities and a company can be found liable for the criminal acts of its officers. Section 18(c) of the Interpretation Act 2005 provides that the term 'person' when used in legislation includes a corporate, unless otherwise specified. Companies can also be vicariously liable for the conduct of employees. Where the doctrine of vicarious liability does not apply, the state of mind of an employee can be attributed to the company in circumstances in which the human agent is the 'directing mind and will' of the company, or when an individual's conduct can be attributed to the company under the particular rule under construction. A company can also be guilty of a strict liability offence, which is an offence that does not require any natural person to have acted with a guilty mind, such as health and safety legislation infringements. Since its commencement on 30 July 2018, this is now also an offence under the Criminal Justice (Corruption Offences) Act 2018.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

An Garda Síochána (the Irish police) is the primary body with responsibility for the investigation and prosecution of crime in Ireland, with a specialised wing for complex fraud-type offences (the GNECB). There are also a number of regulatory bodies with a separate specific remit to investigate and enforce corporate crime. These types of investigations are often carried out with the assistance of the police. The regulatory bodies include:

- the ODCE, which monitors and prosecutes violations of company law;
- the Office of the Revenue Commissioners (the Revenue Commissioners), which is responsible for the collection, monitoring and enforcement of tax laws;
- the Competition and Consumer Protection Commission (CCPC), which is responsible for competition law and consumer protection;
- the Central Bank of Ireland (CBI), which regulates financial institutions;
- the Health and Safety Authority, which enforces occupational health and safety law; and
- the Data Protection Commission (DPC), which is responsible for data protection law.

In terms of prosecution, offences are divided between summary (minor) offences and indictable (serious) offences. In general, regulatory bodies, such as those listed above, are authorised to prosecute summary offences directly. The Office of the Director of Public Prosecutions (DPP) is the relevant body for the prosecution of criminal offences on indictment, or for prosecution of summary offences outside the remit of regulatory bodies. The DPP has no investigative functions; the relevant investigating body prepares a file and submits it to the DPP for consideration. It is then solely at the discretion of the DPP as to whether a case will be taken.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

This will depend on the statutory basis for that investigation. For the most part, investigations are initiated on the basis of a complaint alleging that an offence has been committed. Some bodies (such as the Standards in Public Office Commission) can only initiate investigations following receipt of a complaint alleging that an offence has been committed, whereas others, such as the DPC, can also initiate investigations on their own initiative. Different bodies use different factors to consider whether to initiate an investigation into a specific matter. For example, the GNECB has stated that it will assess whether to investigate a complaint on the basis of different factors, such as the monetary loss involved, the international dimension of the complaint and the complexity of the issues of law or procedure that arise.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

The lawfulness or scope of a notice or subpoena from a law enforcement authority may be challenged in the Irish courts through judicial review proceedings. However, it may be possible to reach a compromise with the law enforcement agency on the scope of the notice. It may also be possible to obtain an interim injunction in certain circumstances preventing the exercise of the notice, subpoena or warrant, or preventing the authority from using information already obtained, unless and until the court determines that the validity of the instrument is valid and enforceable.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Irish law does not recognise plea bargaining or co-operative agreements. The decision to prosecute is at the discretion of the DPP and the courts have discretion in imposing sentences within the statutory minimum and maximum periods.

7 What are the top priorities for your country's law enforcement authorities?

Regulatory bodies typically publish their enforcement priorities annually. The CBI's priorities include, among other things, outsourcing by financial firms, MiFID implementation, fintech, conduct, behaviour and culture of regulated entities, money laundering and counter-terrorist financing compliance, while the DPC and the CBI have both stated that their current focus is on cybersecurity.

As mentioned in question 1, the Irish government has a specific renewed focus on tackling white-collar crime. A key part of its efforts in this space was the introduction of the Criminal Justice (Corruption Offences) Act 2018, plans to establish the ODCE as an independent company law compliance and enforcement agency, and piloting a Joint-Agency Task Force to tackle white-collar crime. The government also intends to enact the Criminal Procedure Bill, the aim of which is to streamline criminal procedures to enhance the efficiency of criminal trials.

The CBI, in collaboration with the Dutch Central Bank, conducted an assessment of the behaviour and culture in five Irish retail banks. In July 2018, it published the findings of this review. As part of these findings, the CBI has proposed the introduction of a new individual accountability framework, which would apply to banks and other regulated financial service providers. The framework includes conduct standards for regulated financial services providers and the staff working in them, a senior executive accountability regime, and enhancements to the existing fitness and probity, and enforcement processes. This is a top priority for the CBI and a consultation paper is expected imminently.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018, which were introduced in September 2018, impose requirements on operators of essential services (OESs) and digital service providers (DSPs) to manage the risks to the security of network and information systems. OESs include operators within specified sectors, including energy, transport, banking, financial market infrastructures, health and digital infrastructure. DSPs are those who provide digital services, including online marketplaces, online search engines and cloud computing services. There is a centralised computer security incident response team in the Department of Communications, Climate Action and the Environment, which both OESs and DSPs must notify if there are incidents that have a significant or substantial impact on these services. The CBI also takes enforcement action against any financial service provider whose failings in cybersecurity cause it to breach its regulatory requirements. For example, in June 2018 the CBI sanctioned an asset management firm for exposing itself to cyber-fraud, which resulted in the loss of €650,000 in client funds. This was the first such enforcement action of its kind.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The Criminal Justice (Offences Relating to Information Systems) Act 2017 was the first Irish legislation to specifically address the issue of cybercrime. The Act created new dedicated cybercrime offences, including:

- accessing or interfering with an information system without lawful authority;
- interfering with data without lawful authority;
- interfering with the transmission of data without lawful authority; and
- use of a computer or data for the purpose of the commission of any of these offences.

The Criminal Justice (Theft and Fraud Offences) Act 2001 also provides that it is an offence to use a computer with the dishonest intention of causing a loss to another person.

As outlined in question 3, An Garda Síochána, the country's national police force, have a specialised division called the Garda National Cyber Crime Bureau, which investigates and enforces cybercrime. Any prosecutions for cybercrime are managed by the DPP.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In general, Ireland does not assert extraterritorial jurisdiction in respect of acts conducted outside the jurisdiction. However, extraterritorial jurisdiction is conferred by statute in respect of specific offences to varying degrees. For instance, section 4 of the Competition Act 2002 provides that it is an offence to be party to an anticompetitive agreement that has the effect of preventing, restricting or distorting competition in trade in goods or services within the state. Importantly, section 4 is not restricted to agreements made within Ireland.

Examples of specific offences for which Ireland exercises extraterritorial jurisdiction are as follows.

Corruption

The Criminal Justice (Corruption Offences) Act 2018 prohibits bribery offences occurring outside Ireland in two sets of circumstances: (1) if an Irish person or company does something outside Ireland that, if done within Ireland, would constitute an offence under the corruption legislation, that person is liable as if the offence had been committed in Ireland; and (2) if an offence under the corruption legislation takes place partly in Ireland and partly in a foreign jurisdiction, a person may be tried in Ireland for that offence. There is no requirement that the offending act should also be an offence in the foreign jurisdiction where the offending act took place. To date, there have been no prosecutions in Ireland under these extraterritorial provisions.

Money laundering

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) (the CJ(MLTF) Act) sets out specific circumstances in which an action can be taken for money laundering occurring outside Ireland. If an individual or a company engages in conduct in a foreign jurisdiction that would constitute a money laundering offence both under the CJ(MLTF) Act and in that foreign jurisdiction, they can be prosecuted in Ireland. This extraterritorial jurisdiction may only be exercised if the individual is an Irish citizen, ordinarily resident in the state, or the body corporate is established by the state or registered under the Companies Act 2014.

The Proceeds of Crime Acts

Under the Proceeds of Crime Act 2016 (the PCA Act), the Irish High Court can make orders depriving a defendant of assets that are merely suspected of being the proceeds of crime, regardless of whether the defendant has been convicted of a criminal offence. The standard of

proof required to determine any question arising under the PCA Act is that applicable to civil proceedings. 'Property' in relation to the proceeds of crime is broadly defined and includes money and all other property, real or personal. 'Proceeds of crime' for the purposes of the PCA Act means any property obtained or received at any time by, or as a result of, or in connection with criminal conduct. The definition of 'criminal conduct' is such that foreign criminality is covered by the scope of the act where the proceeds are within the state. Therefore, the legislation has extraterritorial effect when (1) the criminal conduct occurred outside the state, but the respondent and the property are situated within the state, provided that the conduct constituting the offence is also an offence in the foreign state, (2) the respondent is situated within the state and the criminal conduct occurred outside the state and the property is located outside the state, or (3) the property is located within the state, the respondent is situated outside the state and the criminal conduct occurred outside the state, provided that the conduct constituting the offence is also an offence in the foreign jurisdiction.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Cross-border investigations, whether by law enforcement, regulators or internal investigations by companies, pose challenges in every jurisdiction for practical, political and legal reasons. For investigations by Irish regulators and law enforcement agencies, the foremost consideration will be whether there is an existing framework for co-operation between Ireland and the other jurisdiction or jurisdictions. The Criminal Justice (Mutual Assistance) Act 2008, as amended, is the primary piece of legislation governing mutual legal assistance between Ireland and other countries. The extent of available co-operation under mutual legal assistance procedures is dependent on the identity of the corresponding state, and the greatest level of co-operation is among other EU Member States. Co-operation with third countries (i.e., those outside the European Economic Area) is dependent on their ratification of relevant international agreements or the existence of a mutual assistance treaty agreed between them. Regulators and law enforcement can co-operate with their counterparts outside these formal procedures, and this will depend on the relationships between such bodies.

Investigations by regulators or law enforcement and by corporations can also encounter difficulties owing to different legal standards. For example, data protection laws in some countries can restrict the flow of information out of the country, and different levels of protection for private data may restrict the possibility of transfer between the jurisdictions. Further, different rules can apply to matters such as the application of privilege and the constitutional protections owed to persons under investigation.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The long-established principle of double jeopardy applies in Ireland. A corporation cannot be prosecuted twice for the same or similar offences on the same facts following a legitimate acquittal or conviction by an Irish court or by a court of competent authority in a foreign jurisdiction. There must be identity between the foreign and domestic offences. It is possible for the same course of conduct in an international setting to give rise to multiple separate offences in different jurisdictions.

The fact that a corporation entered into a deferred prosecution agreement (DPA) in a different country is unlikely to prevent prosecution in Ireland, which does not provide for the use of DPAs, unless the DPA was viewed as being equivalent to an acquittal or conviction.

Typically, the principle does not apply until proceedings are concluded. However, under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended), no proceedings may be initiated in circumstances where an individual has been charged under that Act in the absence of consent from the DPP.

There is no anti-piling on policy in Ireland that prevents multiple enforcement authorities from taking action against an entity in relation to the same conduct.

13 Are 'global' settlements common in your country? What are the practical considerations?

It is possible for a domestic authority to reach a resolution as part of a coordinated approach with an overseas authority. However, if a party wishes to reach a settlement with authorities in another country or countries, it should be aware that such an agreement may not prevent Irish authorities from continuing to pursue a prosecution.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Investigations into similar matters in other jurisdictions are often the catalyst for investigations in Ireland. Irish authorities will usually try to co-operate with foreign investigation authorities, and the exchange of information through appropriate channels can aid an investigation greatly. Irish investigatory authorities will take notice of decisions made by foreign investigatory authorities, but the weight given to such a decision will vary depending on factors such as the similarity of the facts under investigation and the jurisdiction concerned. Ultimately, it will be a matter for the Irish authorities to determine whether and how to conduct their own investigations, and prosecutions and enforcement actions in other jurisdictions will at most be one of a number of factors considered.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

While sanctions are imposed at an international level, they are implemented at a national level. Therefore, individuals and companies operating in Ireland should be aware of the restrictions imposed under Irish law that implement international sanctions. As a Member State of both the United Nations and the European Union, Ireland is required to observe and enforce UN Security Council sanctions and EU restrictive measures. Each Member State is required to designate their competent authorities that are engaged with sanctions issues. In Ireland's case, these are the Department of Foreign Affairs and Trade, the Department of Business, Enterprise and Innovation and the CBI. The competent Irish authorities are not responsible for designating sanctions against individuals or other states. The competent authorities enact legislation that enforces sanctions imposed by either the European Union or the United Nations. For example, the Department of Business, Enterprise and Innovation implements trade sanctions issued by the United Nations and the European Union, and the CBI handles all financial sanctions. The CBI's website includes up-to-date information on the most recent EU financial sanctions and UN targeted financial sanctions.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

As outlined in question 15, sanctions are implemented at a national level. The CBI is responsible for ensuring that regulated entities operating in the financial services sphere in Ireland comply with financial sanctions. Any regulated entity in Ireland could find itself subject to enforcement action in respect of policies and procedures around financial sanctions screening.

Sanctions enforcement activity in recent years has increased on account of the European Union being more proactive in imposing sanctions. For example, in recent years, the emergence of ISIL as a terrorist threat, the sanctions imposed on Russia after the annexation of the Crimean peninsula and the ongoing conflict in Syria have all resulted in increased sanctions activity, with which Irish companies are obliged to comply. While several enforcement settlements issued by the CBI have to date related to anti-money laundering failures, there have been no settlements yet specifically related to failures concerning a firm's financial sanctions screening process.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Coordination and co-operation between competent authorities of each Member State is facilitated through the implementation of EU and domestic legal instruments. This ensures efficient national coordination and communication mechanisms between all relevant competent authorities.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

As a member of the European Union, Ireland is subject to the EU Blocking Regulation, which was expanded in August 2018 to curtail the effects of the United States' withdrawal from the Joint Comprehensive Plan of Action. The Regulation effectively nullifies the extra-territorial application of the US sanctions against Iran by prohibiting compliance with any sanctions imposed by the United States; preventing the enforcement of any judgment from a foreign court outside the European Union that gives effect to the sanctions; by requiring any EU person, natural or legal, to notify the European Commission of any effects that the sanctions may have on them; and by allowing any EU person to seek compensation caused by the application of the sanctions.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

The Irish courts implement certain aspects of the EU Blocking Regulation by not enforcing or recognising any judgments that may be made outside the European Union. Further, the courts will allow EU persons to seek compensation in the Irish court system for any adverse effects caused by the application of US sanctions.

Under SI 217/1997 (European Communities (Extraterritorial Application of Legislation Adopted By a Third Country) Regulations), failure to comply with the EU Blocking Regulation is an offence and may be punished by a fine or up to 12 months' imprisonment.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

- Allegations of misconduct will often by raised by whistleblowers, who are protected by the Protected Disclosures Act 2014. Accordingly, great care must be taken not to violate these protections when allegations come to light in this way. Under the Central Bank Act (Supervision and Enforcement) Act 2013, there are specific whistleblower protections in relation to making disclosures to the CBI when breaches of financial services legislation may be in issue.
- Thematic reviews are typically carried out by regulators. By the time an allegation of misconduct has arisen on a thematic review or as a result of any other regulatory oversight, the company may not be able to remedy the matter or otherwise prevent an investigation or enforcement action. For example, the CBI often bases its investigations on the Administrative Sanction Procedure under the Central Bank Act 1942 (as amended) on matters identified during thematic reviews.
- When allegations arise through media reports, publicised litigation or other publicised external sources, there are more immediate public relations risks than when a matter arises internally. Companies should consider engaging a public relations agency if there are significant reputational risks attached to any allegation of misconduct.
- There are specific legislative provisions that oblige persons to report information in relation to certain offences in certain circumstances. The Supreme Court recently upheld the

enforceability of section 19 of the Criminal Justice Act 2011 in *Sweeney v. Ireland* [2019] IESC 39. If a company is a regulated entity, it may be required to make certain disclosures to its regulator, or indeed to self-report unintentional breaches or offences. Auditors have disclosure obligations, and misconduct coming to light during their engagement may trigger a reporting obligation.

- There is political appetite to ensure Ireland remains an attractive location in which to do business. The introduction of the 'corporate offence' in the Criminal Justice (Corruption Offences) Act 2018 enables a corporate body to be held liable for the corrupt actions committed for its benefit by any director, manager, secretary, employee, agent or subsidiary. The single defence available to corporates for this offence is demonstrating that the company took 'all reasonable steps and exercised all due diligence' to avoid the offence being committed. Although there is no Irish guidance on the legislation yet, 'reasonable steps' could include ensuring measures are taken to promote and ensure a corporate culture of reporting suspicions or concerns in relation to corruption and that any suspicions or concerns are notified and, where appropriate, reported to the relevant authorities.

Information gathering

21 Does your country have a data protection regime?

Ireland's data protection regime mainly comprises the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the Data Protection Acts 1988–2018 (the DP Acts). Within this regime, there are a number of duties on data controllers, including an obligation to process personal data (under the meaning of the GDPR and the DP Acts) fairly, for it to be kept up to date and secure.

Additionally, the Criminal Justice (Offences Relating to Information Systems) Act 2017 (enacted on 24 May 2017) gives effect to provisions of Directive 2013/40/EU on attacks against information systems. The Act introduced a number of criminal offences, including:

- unauthorised access of information systems;
- interference with information systems or with data on such systems;
- interception of the transmission of data to or from information systems; and
- the use of tools to facilitate the commission of these offences.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The DPC is responsible for monitoring the application of the DP Acts and the GDPR to protect the rights and freedoms of individuals in relation to processing.

The DPC has a number of investigative powers, including the power to conduct an audit, the power to compel individuals and companies to provide it with information and documentation, and the power to prohibit the transfer of personal data overseas.

Summary proceedings may be brought and prosecuted by the DPC. In relation to indictable offences, the DPC prepares a file and submits it to the DPP for consideration; it is then solely at the discretion of the DPP as to whether a case will be taken in respect of a suspected offence.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

The GDPR and the DP Acts restrict the use and disclosure of an individual's data in Ireland. There are exceptions to the protection given under the DP Acts, but there is no specific exemption when an internal investigation is being carried out. Therefore, all the rules and protections regarding personal data, as set out in the DP Acts, must be followed during an internal investigation. Traditionally, companies have relied upon consent to support internal investigations; however, the DP Acts now require that consent be freely given to be valid. In the context of employment, there is an inherent imbalance of power between employee and employer. In addition, the GDPR requires that a data subject can withdraw his or her consent at any time. These factors make it difficult for employers, in the majority of circumstances, to rely upon consent as a legal basis for processing data, albeit not impossible.

Companies should therefore seek an alternative lawful basis for processing in the context of internal investigations. The DP Acts allow for data to be processed if it is necessary for the purposes of legitimate interests pursued by the data controller, which can be the case for an internal investigation, but that needs to be balanced against the fundamental rights and freedoms and the legitimate interests of the data subject in question.

Organisations do have a legitimate interest in protecting their business, reputation, resources and equipment. However, Irish law recognises a broad 'right to privacy', which includes a right to privacy at work, and a person does not lose privacy and data protection rights simply by being an employee. Any limitation of an employee's right to privacy should be proportionate to the likely damage to the employer's legitimate interests.

If an employer seeks to use 'legitimate interests' as the basis for processing data, an employee as data subject will have a right to object to that processing of their data. This right is not absolute and may be overridden by the employer having 'compelling reasons' to process the data. The severity of the suspected offence will therefore affect the employer's ability to satisfy this requirement. Companies should also ensure that this balancing exercise between the legitimate interests of the company and those of the employee be carried out prior to conducting the internal investigation, and information in respect of any such exercise should be made available to employees.

In any event, companies must inform their employees of the right to object and should draft an internal investigation policy reflecting this balance. Employees should be notified of the possibility that an investigation might take place and, in particular, the ways in which their personal data might be processed in the context of an investigation. For new employees, this information should be provided when they join the company. However, for existing employees, the provision of an updated internal investigation policy will be sufficient.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Irish employers have the right to monitor employees' communications. However, this is subject to the right to privacy that employees are afforded under both the Irish Constitution and the European Convention on Human Rights, as well as under data protection law. Any intrusion of an employee's right to privacy must be proportionate to any likely damage caused to the employer's legitimate interests.

When an employee wishes to enforce the right to privacy or believes that it is has been infringed, he or she may do so by referring a dispute to the Workplace Relations Commission or by commencing proceedings in the courts. If the dispute involves the employee's personal data, it may be possible to lodge a complaint with the DPC.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants and dawn raids are often used as part of investigations against companies, particularly by the CCPC and the ODCE. Both company premises and private homes of relevant persons can be searched on the basis of an appropriate warrant.

There are constitutional protections for persons subject to searches, particularly of private homes. Depending on the specific statute, a regulator or investigatory body would obtain a search warrant to enter a dwelling to conduct a search and to seize documents. There is a general requirement that there is some nexus between the investigation by the regulatory body of the offence in question and the dwelling in question. The body is only permitted to search the premises specified in the warrant and to seize items coming within the terms of the warrant.

Evidence seized outside the scope of a search warrant may, depending on the circumstances, be inadmissible at trial.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Privileged material is prima facie protected from examination by law enforcement or regulatory bodies. Specific statutes, such as the Companies Act 2014 and the Central Bank (Supervision and Enforcement) Act 2013, also provide for the protection of privileged information during investigations.

In practical terms, it can be difficult to determine during a seizure operation whether material is privileged, and sometimes the material will be isolated so that a claim of privilege can be assessed later.

The mechanism to assess whether privilege has been properly asserted will be dependent on the legislation under which the search warrant was granted. For example, the Competition and Consumer Protection Act 2014 provides a mechanism whereby material that is seized, and is claimed to be legally privileged, is retained and vetted by an independent assessor to determine whether privilege has been properly asserted.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

The Irish Constitution recognises a right to silence and the privilege against self-incrimination. Arrested suspects are brought into police custody for questioning 'under caution'. The suspect

should be cautioned that they have the right to maintain silence and that anything they say may be used in evidence. However, the Criminal Justice Act 1984 (as amended) provides that, in the case of arrestable offences (i.e., those for which a person can be imprisoned for five years or more), inferences can be drawn at trial from an accused's silence.

The right to silence can be abridged by statute, most often in the context of regulatory investigations, meaning that answers can be compelled. However, Irish courts have frequently held that statements given under statutory compulsion (such as in connection with a regulatory investigation attracting a civil penalty) cannot be used against that person in subsequent criminal proceedings, whereas voluntary statements can be.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The Protected Disclosures Act 2014 (the 2014 Act) protects whistleblowers and provides for a tiered disclosure regime with a number of avenues open to whistleblowers. The 2014 Act encourages the vast majority of protected disclosures to be made to the employer in the first instance. However, other options are available if this is inappropriate or impossible.

There are no financial incentive schemes for whistleblowers.

When a worker makes a protected disclosure, the employer in question is prevented from dismissing or penalising the worker, taking an action for damages or an action arising under criminal law, or disclosing any information that might identify the person who made the disclosure. If the employer were to dismiss or penalise a worker wholly or mainly as a result of him or her making a protected disclosure, the worker could be awarded up to five years' remuneration, re-engagement or reinstatement by the Workplace Relations Commission (the employment tribunal in Ireland). Further, the 2014 Act creates a cause of action in tort for the worker for detriment suffered as a result of making a protected disclosure. The definitions of 'protected disclosure', 'relevant wrongdoing' and 'worker' are quite broad, and care should be taken to consider whether the Act applies in every case of reported misconduct.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

As a general matter, employees have a constitutional right to 'fair procedures' in any investigative or disciplinary process. This means that, among other things, the employee must be kept appraised of the investigation and must be permitted to participate in the investigation and make points in their defence. The extent and scope of fair procedures and natural justice that must be afforded during a workplace investigation depends on the actual nature of the investigation and the potential consequences thereof.

The rights do not differ for officers and directors who are employees.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

The rights outlined in question 29 apply in an investigation and disciplinary process when a person is implicated or suspected of having engaged in misconduct.

Prior to a finding of misconduct being made, an investigation and disciplinary process should be carried out.

The disciplinary process should, at a minimum, follow the Workplace Relations Commission's Code of Practice on Disciplinary and Grievance Procedures, the employer's own procedures and involve the basic principles set out below.

- Advance written notice of any allegations, and any supporting documentation and witness statements, should be provided to the employee.
- The employee should be invited, in writing, to an investigation meeting to discuss the allegations and to put forward his or her response.
- The investigation should go no further than to determine whether there is a sufficient factual basis to warrant a matter being put to disciplinary hearing.
- Suspension should only be imposed after full consideration of the necessity for it pending a full investigation of matters. It may be justified if it is to prevent repetition of the conduct complained of or interference with evidence; to protect individuals at risk from such conduct; to comply with any regulatory rule applicable to the individual or their role; or to protect the employer's business and reputation. Suspension must be for no longer than is reasonably necessary and on full pay and benefits.
- Depending on the outcome of an investigation, the employee should be invited in writing to a disciplinary meeting to discuss the allegations and to put forward a response. Documents obtained during the investigation should be provided to the employee.
- The employee should be allowed to bring a colleague or trade union representative to any meetings.
- Any sanction must be proportionate and reasonable in the circumstances and should be confirmed in writing to the employee.
- A right of appeal to someone not previously involved should be provided.
- Unless the allegations are sufficient to constitute gross misconduct, the sanctions should progress from verbal warning to written warning to final written warning to dismissal. Summary dismissal will only be permitted where the circumstances genuinely constitute gross misconduct.

The following specific protections may arise in the context of conduct-related investigations and dismissals.

- Unfair dismissal. In general, an employee with one year of continuous service may bring a claim for unfair dismissal. An employer cannot lawfully dismiss an employee unless substantial grounds exist to justify termination, such as the employee's conduct. Regard will also be given to the reasonableness of the employer's conduct and the extent of any failure to adhere to agreed procedures. A preliminary investigation is an essential precursor to a fair disciplinary process.

- Discrimination. Irrespective of length of service, an employee may bring a claim for discriminatory dismissal or discrimination based on any one of the nine discriminatory grounds contrary to equality legislation (i.e., gender, civil status, family status, sexual orientation, religion, age, disability, race (including colour, nationality and ethnic or national origin) and membership of the traveller community).
- Whistleblowing. See question 28.
- Wrongful dismissal or High Court injunction. An employee can seek a High Court injunction to restrain an employer from implementing a dismissal if the decision is not implemented correctly. An injunction maintains the status quo pending the determination of an overarching breach of contract claim. A similar order may also be brought to restrain an investigation or disciplinary hearing before matters even reach the dismissal stage. A challenge may be based on corporate governance grounds, the fairness of the procedures adopted or failure to terminate the contract in accordance with its terms.

For dismissal for out-of-work misconduct to be deemed fair, there must be a genuine connection between the employee's offence and his or her employment. The connection must be such that it leads to a breach of trust or causes reputational or other damage to the employer. In such circumstances, the employer should carry out its own internal investigation and disciplinary process (in accordance with the requirements set out above).

31 Can an employee be dismissed for refusing to participate in an internal investigation?

The extent to which an employer may take disciplinary action against an employee for failure to participate in an investigation, up to and including dismissal in accordance with its disciplinary procedure, will depend on the circumstances.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

There is no statutory requirement for such a document, but it would be considered general good practice. Depending on the circumstances, it may be useful to detail the purpose and scope of the investigation and to clarify the remit of the investigators' role. Matters to cover might include:

- the structure and methodology of the investigation;
- a definition of the issues to be covered; and
- details of any engagement with legal counsel and related matters concerning privileged material.

If the investigation concerns employees of the company, it should go no further than gathering the relevant information or evidence to determine whether or not there is a sufficient factual basis to put particular allegations at a formal disciplinary hearing. The investigation

should be carried out in accordance with any relevant internal procedures and not reach any factual conclusions on the evidence or decide whether the allegations are proved.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Depending on the severity of the issue, it would usually be prudent for a business to carry out a certain level of enquiry and investigation. However, a company should take care in carrying out any investigations and in creating any reports, as it is possible that any such documents could be subject to disclosure in any subsequent legal proceedings. A company would not generally be obliged to voluntarily provide the results of such an investigation to the relevant authorities unless it is required under a court order, statute or as part of a self-report. A number of legislative provisions impose a positive obligation on persons (including businesses) to report wrongdoing in certain circumstances (see question 50).

It is also essential, of course, that any wrongdoing ceases as soon as the company becomes aware of it, and that remedial measures are taken where appropriate. Care should be taken to preserve evidence of the wrongdoing, as a failure to do so could result in accusations of destruction of evidence, which can itself be an offence under certain legislation, such as pursuant to section 793 of the Companies Act 2014.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

It is advisable to immediately implement a 'document hold' by suspending deletion policies and circulating document retention notices.

The company should review the request and consider the power under which it is exercised, and in particular if the request is voluntary or mandatory. There are risks associated with releasing documentation, particularly when it might contain confidential or personal information, without being lawfully compelled to do so. External legal advice may be required in this regard.

An inventory listing the materials falling within the notice should also be prepared. The material should then be assessed for privilege. Copies of anything provided to the investigation authority should be retained.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Privately owned companies are not required to publicly disclose the existence of internal investigations or contact from law enforcement. There may, of course, be commercial reasons for doing so (or not doing so) in any particular case.

Under the Irish Listing Rules, publicly listed companies on the Irish Stock Exchange (Euronext Dublin) must, without delay, provide to Euronext Dublin any information that it considers appropriate to protect investors. Euronext Dublin may, at any time, require an issuer to publish such information within the time limits it considers appropriate to protect investors or to ensure the smooth operation of the market.

36 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are considered part of good corporate governance. However, companies operating in Ireland can be subject to certain reporting obligations in respect of certain offences and will therefore be required to notify matters to law enforcement or regulators in certain circumstances (see question 50).

The Irish High Court ruled in *Mooney v. An Post* [1998] 4 IR 288 that the acquittal of an employee of criminal charges does not preclude employers from considering whether an employee should be dismissed on the basis of the impugned conduct. However, if criminal prosecution precedes an internal investigation, in general, internal disciplinary procedures are suspended to respect the individual's right to silence.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Any requirement to disclose documents obtained through an internal investigation to the Irish authorities is qualified by legal professional privilege. In Ireland, documentation, including electrical documentation and audio and visual records of communication, may attract legal professional privilege either in the form of legal advice privilege or litigation privilege. Legal advice privilege arises regarding confidential communications between a lawyer and a client that are created for the sole or dominant purpose of giving or seeking legal advice, even if there is no actual or potential litigation. Litigation privilege applies to communications between a lawyer and a client made in the context of contemplated or existing litigation or regulatory action and also covers communications with third parties, such as experts. Litigation privilege can be a broader form of privilege to assert in the context of an internal investigation, provided there is actual or contemplated litigation or regulatory action.

The main way to protect privilege is to involve lawyers in internal investigations at an early stage, although it should be noted that privilege cannot be created regarding existing documents after they have been created merely by involving lawyers. To ensure that existing privilege is not lost, it is important to limit the disclosure or sharing of materials to essential persons only. Legal advice should not be summarised or copied and shared by non-legal persons. If privileged materials need to be shared with third parties, it is important to ensure that appropriate confidentiality agreements are put in place to govern such disclosure and that, as far as possible, privilege is not inadvertently waived or lost.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Legal professional privilege applies equally to individuals and companies and belongs to the client (see question 37). Under Irish law, the question of who is the client in a corporate context was considered in *UCC v. ESB* [2014] IEHC 135. In that case, it was held that if the client is a corporate body, it is necessary to consider whether the individual making the

communication to the lawyer is a person engaged or employed to obtain or receive legal advice on behalf of the client.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Both in-house and external counsel attract legal professional privilege when the criteria for legal professional privilege are met. In-house counsel must be acting in their capacity as a legal adviser and not, say, as an officer of the company. However, the position with regard to in-house counsel in the context of certain external matters is not straightforward and advice should be sought as a result of the decision of the European Court of Justice in *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v. Commission* (Case C-550/07 P).

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

The position in Ireland is that, as far as legal professional privilege is concerned, the definition of 'lawyer' extends to foreign lawyers. There does not appear to be any question about this and it is generally accepted that foreign legal advice is privileged to the extent that it fits Irish legal rules on privilege.

For example, in *Sports Direct International Plc v. Minor & ors* [2015] IEHC 650, the High Court applied privilege to English legal advice without questioning whether it would apply.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Asserting legal professional privilege is a legal right and the fact of its assertion should not be held against a party. However, if the materials regarding which legal professional privilege is being asserted are central to any enforcement investigation (such as a party defending certain conduct on the basis that it was taken following legal advice), it may appear unco-operative to refuse to disclose such material. In such a case, disclosure could, in fact, be in a party's strategic interest. Any decision to waive privilege should be carefully considered as, once waived, legal professional privilege is lost. It is generally recommended that a waiver should be limited to those materials that are strictly necessary and should be made on a limited and specified basis; in other words, a general waiver of all legal professional privilege in respect of a particular matter is not advisable.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

It is possible to waive privilege on a limited basis. However, care should be taken as privilege can inadvertently be lost in such circumstances. The scope of the waiver should be clear, limited and in writing; furthermore, it is of utmost importance that confidentiality in the material should be maintained.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

If the waiver of privilege was appropriate, limited and restricted, it should not defeat the overall assertion of legal professional privilege. However, this will depend on the extent and nature of the waiver in each case.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege does exist in Ireland. It is important that common interest privilege is expressly asserted and that the third party is aware of the necessity of preserving privilege in the materials received, such as by not disclosing it to any other persons outside the common interest circle.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Third-party communications are only protected against disclosure in the context of litigation privilege. Litigation privilege can be asserted regarding third-party communications where the dominant purpose of the communication is in anticipation of existing or contemplated litigation (which currently includes regulatory proceedings).

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Witnesses can be interviewed in internal investigations and are often seen as an integral part of the fact-finding exercise of an investigation. However, the internal investigation would not be able to compel witnesses to attend, except to the extent that employees can be requested to co-operate in the context of their employment.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Reports that contain legal analysis, advice or conclusions, or which are prepared with the dominant purpose of preparing for, or in contemplation of or in connection with litigation or regulatory proceedings, can be protected by legal professional privilege.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

It can be important that witnesses are informed of the nature of the interview, whether they are implicated in any wrongdoing and, crucially, of any possible consequences for them of the investigation process to preserve the ability to take appropriate action, if necessary, following or as a result of the investigation. It is important to note that any lawyers present are acting for the company and not for the employee, who may, in some cases, have his or her own legal representation.

Existing employees have a greater right to fair procedures as they are more likely to face the possibility of an adverse outcome, such as dismissal. However, it is best practice to accord equal, fair procedures to all interviewees.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

It is good practice to ensure that any documents of relevance to the witness are put to them. 'Interview by ambush' is contrary to fair procedures and open to challenge, particularly by employees.

Employees have no statutory right to legal representation at witness interviews. However, if the employee or witness is, or may become, the subject of the investigation, the employer should consider advising the employee or witness to have legal representation to minimise the risk of a later legal challenge to the investigation process. If the person requests permission to have legal representation, the company should assess each case separately. It is generally considered prudent to permit such representation, or not to proceed in the absence of such representation.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

A number of legislative provisions impose a positive obligation on persons (including businesses) to report wrongdoing in certain circumstances. Most significantly, section 19 of the Criminal Justice Act 2011 provides that a person is guilty of an offence if he or she fails to report information that he or she knows or believes might be of 'material assistance' in preventing the commission of, or securing the prosecution of another person in respect of, certain listed offences, including many corporate crimes. The disclosure must be made 'as soon as practicable', and a person who fails to disclose such information may be liable to a fine or imprisonment for up to five years, or both. However, the person considering making the report may need to make enquiries to be satisfied that a report is justified.

The Supreme Court case of *Sweeney v. Ireland, Attorney General and Director of Public Prosecutions* [2019] IESC 39 has important implications for section 19 of the Criminal Justice Act 2011.

In overturning the High Court decision, the Supreme Court upheld the constitutionality of section 9(1)(b) of the Offences Against the State (Amendment) Act 1998. This decision has implications for section 19 of the Criminal Justice Act 2011 (the 2011 Act), which provides that a person is guilty of an offence if he or she fails to report information that he or she knows or believes might be of material assistance in preventing the commission of, or securing the prosecution of, another person of certain listed offences, including many white-collar offences. The wording of section 19(1)(b) of the 2011 Act is identical to that of section 9(1)(b) of the 198 Act except that the former applies to a 'relevant offence' and the latter applies to a 'serious offence'. In finding that the provision was sufficiently certain, the Supreme Court held that the 1998 Act was clear in what it obliges witnesses to do – to

disclose information pertaining to serious offences that they know will aid in the prosecution of such an offence. Although the Supreme Court noted that no comment has been made as to the constitutionality of similar provisions, such as section 19(1)(b) of the 2011 Act, it would appear to indicate that such reporting obligations would be likely to withstand a similar legal challenge.

Other mandatory reporting obligations include the duties of:

- persons with a 'pre-approved control function' to report breaches of financial services legislation;
- designated persons (auditors, financial institutions, solicitors) to report money laundering offences;
- auditors to report a belief that an indictable offence has been committed;
- auditors or persons preparing accounts to report theft and fraud offences; and
- all persons to report any offence committed against a child.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

A company might be advised to self-report, in Ireland or overseas, to mitigate the risk of prosecution or any potential sentence that may be imposed by a court. There are no express provisions for immunity or leniency in prosecution under Irish law, but self-reporting can be considered a mitigating factor in sentencing. The DPP does have discretion to grant immunity in certain circumstances. Some regulatory regimes, such as the CBI's administrative sanction procedure, also consider self-reporting as a mitigating factor affecting the level of sanctions. The list of sanctioning factors set out in the CBI's Administrative Sanctions Procedure (published in 2018) includes 'how quickly, effectively and completely the regulated entity brought the contravention to the attention of the CBI or any other relevant regulatory body'.

The exception is the Cartel Immunity Programme operated by the CCPC, which allows a member of a cartel to apply for immunity in return for co-operating with the CCPC. Only the first member of a cartel to come forward can avail of the programme and must meet strict eligibility criteria.

In terms of extraterritorial self-reporting, an Irish company may self-report to authorities in other jurisdictions that have immunity or leniency programmes if the conduct in question could also be investigated or prosecuted by those authorities. For example, the European Commission runs a cartel immunity programme and an Irish company may self-report to the Commission to avail of this.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

It is important that a company has considered its risks and, as far as possible, investigated the matter before making a report. A report can be made in writing, such as by letter to the appropriate authority, or by providing a written statement upon attending a Garda station. The form and content of the report will depend on the specific circumstances of the matter, including, for example, whether the company might be implicated, or whether there are

other legal, commercial or reputational issues to be considered. Data deletion policies should be suspended and relevant materials retained in case they are subsequently required in the context of an investigation or legal or regulatory proceedings.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Dialogue may start with the authority once a notice has been received and analysed. For example, the company may wish to address concerns such as the scope of the request, the legal basis or the deadline for compliance. It is important that care is taken with such communications, as they can set the tone for engagement with the authority and may be relevant for any subsequent court challenge or dispute that may arise.

54 Are ongoing authority investigations subject to challenge before the courts?

Ongoing investigations may be subject to challenge in the courts, for example through an application for judicial review. It is also possible to seek injunctions, typically on an interim basis, to protect legal rights while the underlying challenge is resolved.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Each request should be treated separately as the legal basis for the request is likely to be different. A request that may appear to compel disclosure of documents may not in fact have legal effect if it is from outside the jurisdiction and the procedures for compelling cross-border information (such as the procedures under the Criminal Justice (Mutual Assistance) Act 2008, as amended (see question 57)) are not engaged. It is generally not advisable to release information, particularly personal data within the meaning of the DP Acts, in the absence of lawful compulsion. 'Package disclosures' are therefore usually unadvisable, as documents that one agency has a legal right to obtain may not be within the compulsory power of another agency. That said, where requests are made by different authorities, it is important to have a consistent approach with regard to how requests are treated and what arguments are made to authorities.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

The appropriate response will depend on the nature of the request and the relationship between the company that is subject to the request and the entities holding the documents across borders. If the company in receipt of the request has the power to compel production,

such as from a branch or subsidiary, it may be required to do so. However, generally, the entity to which the request is addressed will be the only body with an obligation to respond.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Irish law enforcement and regulatory bodies are known to share information informally with equivalent bodies in different jurisdictions.

In terms of formal co-operation mechanisms, the Criminal Justice (Mutual Assistance) Act 2008 gives effect to 12 international agreements that establish the existing legislative framework for the provision of mutual legal assistance. The Criminal Justice (Mutual Assistance) (Amendment) Act 2015 gives effect to a further six international instruments not provided for by the 2008 Act. This has enhanced the already significant level of co-operation between Ireland and other EU Member States. Co-operation with third countries (those outside the European Economic Area) is dependent on their ratification of relevant international agreements or the existence of a mutual assistance treaty agreed between them.

The transposition of the EU Fourth Money Laundering Directive into Irish law has also led to further enhanced international co-operation, as the Directive requires information to be shared between competent national authorities, including the creation of a central register of beneficial owners of entities.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

There is no generally applicable statutory obligation that creates an obligation on the police to keep information received during an investigation confidential.

Irish law does recognise a broad 'right to privacy', however, which is protected by the Irish Constitution, the EU Charter of Fundamental Rights and the European Convention on Human Rights. Further, data protection is regulated in Ireland primarily by the DP Acts. Irish data protection laws reflect EU data protection laws and protect the personal data of individuals from disclosure in certain circumstances. The police are subject to the same obligation under the DP Acts as all 'data controllers', within the meaning of the DP Acts, when processing personal data. There are exceptions to the rules set out in the DP Acts, including where the processing is required to investigate or prevent an offence.

The police may disclose information to law officers and other law enforcement agencies during an investigation or on the basis of the prevention and detection of offences, under mutual assistance agreements with Interpol Europe and other agencies that have a statutory investigative and enforcement role.

Whistleblowers are protected from identification by the Protected Disclosures Act 2014. Accordingly, great care must be taken not to violate these protections when an investigation involving whistleblower information is under way. However, the identity of whistleblowers can be disclosed to prevent a crime or to aid in the prosecution of a criminal offence.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

In such circumstances, it would usually be prudent to advise the company not to provide the documents. However, the company should ensure that it is not violating any laws in its own jurisdiction by doing so. The company should inform the requesting authority of the basis for the decision to refuse the request for documents.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Data protection is regulated in Ireland primarily by the DP Acts. Irish data protection laws reflect EU data protection laws and protect the personal data of individuals from disclosure in certain circumstances. The transfer of data outside Ireland is restricted, but there is no outright 'block' preventing all transfers. The main implication of Irish data protection law is that companies may be reluctant to release materials in the absence of a legal obligation.

As discussed in question 23, Irish law also recognises a broad right to privacy, which can restrict the disclosure of data even when the disclosure would comply with the DP Acts.

Further, care should be taken when releasing documents that relate to any type of contractual relationship, as there may be confidentiality terms in the contract or engagement terms that could be violated by the disclosure. A party should always be mindful that if it releases information without being compelled to do so, it is not protected from claims that it has breached Irish data protection legislation or breach of confidence claims.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

As outlined in questions 59 and 60, there are risks attached to voluntary production of documents, and it is generally not advised unless there are compelling reasons to do so. In particular, as noted in question 58, a company may be in breach of the DP Acts if it releases materials that contain personal data in the absence of lawful compulsion, and may also be in breach of confidence if it releases confidential material without being compelled to do so. There may also be other contractual consequences for a company releasing certain materials voluntarily. There is no automatic confidentiality attached to materials disclosed to law enforcement, unless restrictions have been agreed to that effect. Accordingly, material provided to authorities voluntarily may be shared with other authorities or used for purposes other than the initial basis of the request. Materials obtained on the basis of a compulsory power are subject to greater protections. However, once material is in the possession of an authority, there is nothing to prevent a third party from seeking the material, such as through a non-party discovery order.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Irish criminal legislation typically provides for monetary fines or terms of imprisonment for offences. Given the nature of corporate entities, the most common form of sanction is a fine. However, while less common, Irish legislation also provides for specific remedies, such as compensation orders and adverse publicity orders under health and safety legislation.

Common sanctions in the context of business crime are restriction and disqualification orders. Under section 839 of the Companies Act 2014, if a person has been convicted of an indictable offence in relation to a company, or convicted of an offence involving fraud or dishonesty, that person may not be appointed to, or act as, an auditor, director or other officer, receiver, liquidator or examiner or be in any way, whether directly or indirectly, concerned or take part in the promotion, formation or management of any company.

As discussed further under question 63, companies convicted of certain offences may be excluded from participation in public tenders for a specific period.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

The EU Public Sector Procurement Directive (2014/24/EU) was transposed into Irish law by the European Union (Award of Public Authority Contracts) Regulations 2016. Under these Regulations, companies must be excluded from public procurement for a specific period when they have been convicted of certain offences. The Regulations also provide for offences that carry discretionary debarment. These include offences under EU law, meaning that a company should take care when settling charges in another country, as doing so could, depending on the offence, trigger these exclusion rules.

The Regulations enable companies to recover eligibility to bid for public contracts by demonstrating evidence of 'self-cleaning', such as the payment of compensation to the victim, clarification of the facts and circumstances of the offence, co-operation with the investigating authority, and the implementation of appropriate measures to prevent further criminal offences or misconduct.

64 What do the authorities in your country take into account when fixing penalties?

Sentencing of corporate crimes is largely a function for the courts. There is no express provision under Irish law for immunity or leniency in prosecution. If a business is found guilty of an offence, a wide range of factors may be taken into account at the discretion of the court. Mitigating factors include whether the company ceased committing the criminal offence on detection or whether there were further infringements or complaints; whether remedial efforts to repair the damage caused were used by the company; the existence of a compliance programme; and whether the company itself reported the infringement before it was detected by the prosecuting authority. Additionally, in imposing any sentence, the court must comply with the principle of proportionality as set out in *People (DPP) v. McCormack* [2000] 4 IR 356.

Certain sanctions, such as those available to the CBI under the administrative sanction procedure or the CCPC in connection with cartels, can be expressed as a percentage of turnover. This allows the size of the entity to be considered when penalties are imposed.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Non-prosecution agreements and deferred prosecution agreements are not available in Ireland. There has been some consideration of these types of arrangements at policy level; for example, the Law Reform Commission (LRC) has recommended in its Report on Regulatory Powers and Corporate Offences (published on 23 October 2018) that deferred prosecution agreements (DPAs) be introduced, based on the UK model, which are subject to court approval. In the United Kingdom, the court must be satisfied that (1) the terms of a DPA are fair and proportionate and (2) a DPA is in the interests of justice before it is approved. Although any recommendations of the LRC are not always followed or implemented, they are usually given serious consideration by the Irish government.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Non-prosecution agreements and DPAs are not currently available in Ireland.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

It is possible to enter into a settlement with some regulatory authorities in prescribed circumstances. For example, the CBI commonly uses settlements to resolve investigations brought under the Administrative Sanctions Procedure under the Central Bank Act 1942 (as amended) (in respect of civil sanctions only). In addition, pursuant to the Cartel Immunity Programme, a settlement may be achieved in specific circumstances.

Generally, any company considering entering into a settlement with a regulatory or enforcement authority should balance the seriousness of the charge, the scope of a conviction and the strength of the case against it, against the terms of the settlement, such as the quantum of any fine and whether there is publicity associated with the settlement. Care should be taken with regard to a settlement under the Cartel Immunity Programme to ensure that the stringent eligibility criteria are met before engaging with the CCPC.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

As DPAs and non-prosecution agreement are not currently available in Ireland, the use of external corporate compliance monitors is not an enforcement tool used by Irish law enforcement authorities. In its Report on Regulatory Powers and Corporate Offences, the LRC

has indicated that the detailed procedures concerning DPAs are best left to be determined in a Code of Practice to be developed by the DPP, comparable to the DPP's Guidelines for Prosecutors and the DPP's Guidelines for the Cartel Immunity Programme.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

A defendant may be subject to simultaneous civil and criminal proceedings arising out of the same set of circumstances. There is no obligation on the courts to adjourn the civil proceedings pending the completion of the criminal proceedings. However, civil proceedings are commonly adjourned pending the outcome of the criminal case. As there are different burdens of proof in civil and criminal matters, the outcome of civil and criminal proceedings will not necessarily be the same. It is also possible, although rare, for individuals to initiate private criminal prosecutions by issuing a summons pursuant to the Petty Sessions (Ireland) Act 1851 in certain limited circumstances.

Authorities are not obliged to disclose their files to such persons unless the particular file is generally open to the public or a court order has been obtained.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

The Irish judiciary is extremely protective of the accused's right to a fair trial and will prohibit or stay a trial if necessary. This sometimes occurs in respect of high-profile cases when the extent of publicity affects the ability of the defendant to have a fair jury trial. An example of this is the trial of a high-profile former chairman of Anglo Irish Bank, which was adjourned in October 2015 and initially rescheduled for seven months later, owing to concerns of adverse publicity surrounding the trial.

Reports that undermine legal proceedings can amount to contempt of court. Further, any reporting that goes beyond a faithful account of the court proceedings could give rise to defamation claims.

Pursuant to the Data Protection Act 2018, new court rules have been introduced to allow access to documents on court files. Under these new rules, an accredited member of the press may access documents that are 'opened' in court (i.e., read out in court by a lawyer or by the judge) and those that are 'deemed to have been opened' at a hearing before the court (i.e., documents that the judge has read in chambers and does not require the parties to formally open in court).

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

In larger companies, corporate communications are generally managed by a team of marketing professionals, and it is common for companies to employ public relations companies when there is a risk of negative publicity.

72 How is publicity managed when there are ongoing related proceedings?

It is important that any public statements issued by a company do not potentially prejudice current criminal proceedings or investigations. Statements issued by a company in such circumstances should be brief, factual and approved by the company's legal advisers. Care should also be taken that no comments are made that potentially identify any persons, as there could be a risk of defamation proceedings if the statement incorrectly implies that the person has committed any wrongdoing.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

As discussed in question 35, Euronext Dublin may require an issuer to publish information within such time limits as it considers appropriate to protect investors or to ensure the smooth operations of the market.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Following the publication in November 2017 by the Irish government of its Measures to Enhance Ireland's Corporate, Economic and Regulatory Framework, aimed at strengthening Ireland's response to corporate misconduct, there have been a number of key legislative changes including:

- the enactment of the Criminal Justice (Corruption Offences) Act 2018, which commenced on 30 July 2018 and effectively repealed and replaced the seven existing Prevention of Corruption Acts 1889 to 2010 into a single statute; and
- the publication in December 2018 of the General Scheme of the Companies (Corporate Enforcement Authority) Bill 2018. This Bill proposes that the ODCE will be re-established as an agency, in the form of a commission, which will be known as the Corporate Enforcement Authority.

As referenced in question 1, the Minister for Justice and Equality appointed Mr James Hamilton, former DPP, to chair a review of Ireland's anti-corruption and anti-fraud structures and procedures in criminal law enforcement in 2018. In March 2019, the review group issued a call for submissions on a number of issues under its terms of reference, which could result in further legislative changes being introduced. The deadline for submission was 19 April 2019 and the results have yet to be published online.

19

Italy

Enrico Di Fiorino[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Based on publicly available information, the highest-profile corporate investigations in Italy focus on international corruption involving the most important Italian companies, infiltration of organised crime in the economic sector and investigations against corporate giants for tax evasion. Italian criminal counsels observe, in particular, the increased focus on regulatory topics, increasing the number of dawn raids with a focus on the internal audit departments of companies, the frequent use of precautionary measures and a growing involvement in cross-border investigations.

2 Outline the legal framework for corporate liability in your country.

While the Italian system has always recognised a civil and administrative liability for companies, only in 2001 did it provide for criminal liability in relation to companies.

This criminal liability is triggered if criminal offences included in a compulsory list have been committed by persons holding representative, administrative or (de facto) managerial positions in the company, or by persons working under their control, provided that these persons have committed the crimes at least 'also' in the interests, or for the benefit, of the company, and the company cannot demonstrate that it has taken adequate measures to prevent the commission of such crimes (in particular, for not having implemented an adequate organisation model or an internal control system).

Foreign companies can also be held criminally liable for crimes committed in Italy, irrespective of whether the laws of the companies' home country contain similar rules or not.

1 Enrico Di Fiorino is a partner at Fornari e Associati.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Several law enforcement authorities regulate corporations in Italy, including the Prosecution Service and independent administrative authorities.

While the Prosecution Service has exclusive jurisdiction on investigations in relation to criminal matters, the independent administrative authorities, which have investigative powers and the power to impose sanctions, only have jurisdiction in specific matters, provided for by law.

As there are several enforcement authorities, the policies and protocols in this regard can differ. However, it is important to highlight that authorities usually have specific protocols relating to co-operation and the exchange of information.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

While the law does not provide for a threshold of suspicion necessary to trigger an investigation carried out by some independent administrative authorities, the public prosecutor shall immediately enter in the dedicated register any criminal data he or she receives or acquires and then start a criminal investigation. The duty of the public prosecutor to bring criminal action is compulsory (and not discretionary).

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Depending on the authority and type of notice, a company may challenge the lawfulness or scope of the notice or production order by way of an application to court.

As regards criminal proceedings, the lawfulness and the scope of a search warrant, and the production of documents or a seizure, may be challenged before the courts. However, subpoenas regarding summoning of witnesses are not challengeable themselves. Witnesses have a duty to testify in front of a judge.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Italian law does not provide for a general application of immunity or leniency in recognition of co-operation with investigative authorities.

As regards criminal proceedings, Italian law has provided several case examples of leniency for specific offences, such as criminal organisation and drug trafficking, and – more recently – immunity (for example, with regard to fiscal-related offences in the case of a voluntary collaboration procedure).

A new law (Law No. 3 of 9 January 2019, Measures to Combat Crimes Against the Public Administration, as well as on the Statute of Limitations for Crimes and the Transparency of Political Parties and Movements) has introduced a new cause of immunity concerning crimes against the public administration, aimed at exempting from punishment anyone voluntarily

reporting the fact within a set amount of time and providing useful and concrete indications to ensure the proof of the crime and to identify the others responsible.

7 What are the top priorities for your country's law enforcement authorities?

The fight against national and international corruption has been a top priority for the Italian government and its law enforcement authorities (in particular, the National Anti-corruption Authority) for the past few years.

Tax evasion is also a key priority. As a result of the changing international situation, Italy developed a parallel domestic strategy aimed at combating tax elusion and tax evasion by means of the signing of bilateral agreements with well-known tax havens, the introduction of the crime of self-money laundering, and the possibility – for a limited amount of time – of voluntary disclosure.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

During the past 20 years, a broad framework of laws has been developed (often as a result of international regulations). In particular, Italy has recently implemented the General Data Protection Regulation (GDPR), which concerns the protection of individuals with regard to the processing of personal data and the free movement of such data, and Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across Europe (known as the NIS Directive).

Criminal offences have been provided in the case of failure to comply with the security measures set out by the law and regulations issued by the Personal Data Protection Authority, unlawful data processing and any untrue or false statement sent to the Authority.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Italian law provides for a wide range of offences to prevent cybercrime. For example, the law punishes the conduct of hacking, phishing, infection of information technology systems with malware, possession of hacking tools, identity theft and electronic theft.

Over the years, the law enforcement authorities (in particular, the Prosecution Service and the Personal Data Protection Authority) have given substantial attention to cybercrime, having acknowledged that the insufficient investment in cybersecurity in Italy risks seriously affecting the country's growth and development.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Italian criminal law provides that Italian courts have jurisdiction on all offences committed within the Italian territory (that is, when at least a part of the prohibited conduct takes place in Italy).

Italy does not have general extraterritorial jurisdiction, although there are specific cases in which it will exercise extraterritorial jurisdiction (e.g., bribery involving Italian public officials and market abuse on financial instruments admitted on an Italian regulated market, even if these offences are committed abroad).

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The principal challenges in cross-border investigations derive from the need to identify which states have the relevant jurisdiction and then the full co-operation and coordination of actions between the state in charge of the investigations and the other states, or all the competent agencies and organisations involved (e.g., in Europe, Eurojust and Europol).

Co-operation is needed because of the existence of different laws and regulations in all the countries, mostly relating to privacy, professional privilege regimes and labour laws.

To facilitate coordination among (at least) the EU Member States regarding criminal matters, Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters came into effect in May 2017. There are also bilateral and multilateral agreements between Italy and other non-Member States.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Pursuant to the provisions of the conventions to which Italy is a party (given its status as a Member State of the European Union), the international principle of *ne bis in idem* can only be applied in the event of *res judicata* (final judgment). Therefore, there is no prohibition against two criminal proceedings on the same cause of action against the same person or corporation taking place at the same time in two different European countries. At the international level, there is the principle of *lis alibi pendens*, but no specific rules aimed at settling the issue of proceedings pending simultaneously.

At the EU level, Council Framework Decision 2009/948/JHA of 30 November 2009 (adopted by Legislative Decree No. 29 of 15 February 2016) provides for a mechanism of 'consultation' among the Member States with the aim of achieving a consensus on any 'agreed' solution so as to avoid parallel proceedings in different Member States.

There are no measures in Italy that are comparable to the US 'anti-piling on' policy.

13 Are 'global' settlements common in your country? What are the practical considerations?

To date, there have been no global settlements involving Italy. However, Italian law does provide for a specific discipline regarding the execution of decisions of foreign states.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

The Italian Criminal Code provides for judgments issued by foreign authorities to be recognised in relation to specific matters, such as reparation. When there are international agreements for recognition in force between the parties, the Italian Code of Criminal Procedure provides for enforcement in Italy according to Italian law. Moreover, a 2010 law provides for a new type of mutual recognition of foreign criminal judgements, when they order a minimum of three years of detention.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

As an EU Member State, Italy follows its restrictive measures, including the Sanctions Regulation. Further, the EU applies restrictive measures for the purposes of pursuing the specific Common Foreign and Security Policy (CFSP) objectives. These measures are thus binding in Italy, and a breach can result in fines and imprisonment. Specifically, an Italian law issued in 2018 aims to organise and simplify the authorisation procedures for the export of dual-use items and technologies.

The Ministry of Economic Development is the government entity responsible for administrative penalties.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

The Italian authorities do not show a strong interest in the execution of sanctions.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

At the European level, Member States co-operate with each other, for example as regards authorisation for European operators who intend to work in Member States affected by trade embargoes.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Italy has implemented the EU Blocking Regulation, listing all the administrative penalties applicable for breaches of the EU provisions. In particular, a fine of up to €92,962 may be imposed on any operator who is in breach of the provisions of the law, and a fine of up to €46,481.17 may be imposed on any operator who fails to comply with the duty of notification pursuant to the law.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

As far as we are aware, the EU Blocking Regulation has not been subject to any binding judicial interpretation. Moreover, with the exception of the European Commission's non-binding Guidance Note – Questions and Answers: adoption of update of the Blocking Statute, no further official guidance has been adopted at a local level by Italian authorities.

Furthermore, no cases have yet been brought before the national courts.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct could come to light in many ways, but they arise most often through whistleblowers, internal audits and media reports. Following the recent adoption of legislation on whistleblowing, which provides for different measures to protect employees who report an offence within their organisation in both the private and public sectors, it is expected that whistleblowing may become even more common.

Information gathering

21 Does your country have a data protection regime?

The main Italian legislation for the protection of personal data is the Privacy Code, recently amended to adapt it to the changes introduced by the GDPR. Moreover, there are several sector-specific pieces of legislation that could affect a data protection regime, such as the Statute of Workers, Consumer Code and Telemarketing Law, and legislation on whistleblowing.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The Data Protection Code provides for both administrative fines and criminal penalties.

The GDPR introduced an antitrust-type sanction regime with fines of up to 4 per cent of annual global turnover or €20 million, whichever is the greater. A limited number of breaches fall into a lower tier and so are subject to fines of up to 2 per cent of annual global turnover or €10 million, whichever is the greater. Regulators will have a range of other powers and sanctions at their disposal.

One year after the GDPR came into effect, the Personal Data Protection Authority published some key figures concerning its application in Italy. Accordingly, since May 2018: (1) 946 data breaches have been notified, (2) 7,219 complaints have been notified, and (3) 48,591 companies have appointed a data protection officer. The first GDPR fine in Italy was issued in April 2019.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

To be able to conduct effective internal investigations, it is certainly necessary to be aware of the potential conflicts between data privacy concerns and the need for gathering information that implies the processing of employees' personal data. Personal data shall be processed lawfully, fairly and in a transparent manner, and collected for specified, explicit and legitimate purposes.

In addition, in compliance with the principle of data minimisation, it shall be ensured that employees' personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

According to local employment law and the Personal Data Protection Authority, a company is prohibited from mass control and unlimited storage of employees' company emails.

Companies should adopt specific internal guidelines, for approval by trade unions and publicised internally, to enable the employer to carry out controls on employees' internet files and emails, with specific reference to making employees aware of the fact that the employer may execute controls on such data during internal investigations.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

If there are reasonable grounds to believe that the *corpus delicti* (the item on which, or through which, the offence has been committed or the profit made from the crime), or material items related to the crime, are located on a company's premises, a search of those premises could be ordered by the public prosecutor.

At the beginning of the search, the accused and the person who has current access to the premises shall be given a copy of the decree ordering the search, with the notice informing them of their right to be assisted by a trusted person.

In the case of seizure ordered by the judicial authority, the person from whom the objects have been seized and the person who would be entitled to their restitution may submit a request for the re-examination of the seizure decree. The request does not suspend the enforcement of the decision.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

The law provides for a duty to hand documents and documentary evidence to the requesting judicial authority, except if the person who possesses them by virtue of function, job, service or profession declares in writing that they are covered by either public service or professional

secret. The judicial authority shall proceed with the necessary ascertainment if it has reasons to doubt the legitimacy of the declaration and if it cannot proceed without gathering the documents. If the declaration is groundless, the judicial authority shall order the seizure, which can be challenged with a request for the re-examination of the seizure decree.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

A witness is obliged to appear before the court, follow the judicial indications regarding the procedural needs and answer truthfully the questions addressed to him or her.

If a witness fails to appear, the court may order his or her compulsory appearance and that he or she pays a fine and the costs arising from the failure to appear.

A witness is not obliged to testify on facts that could lead to self-incrimination. Moreover, the law provides for a right of abstention for the next of kin of the accused and for persons who invoke either public service or professional secret.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

A whistleblowing law, generally applicable to the private sector in Italy, came into force in December 2017. The protection scheme for whistleblowers provided by the law is applicable only when the company has adopted an organisational model for crime prevention. In all cases, the whistleblower's identity is and must be kept strictly confidential.

There are no incentives provided for in relation to reporting individuals.

However, the whistleblower is protected from any retaliatory or discriminatory dismissal as a consequence of his or her reporting, and protection from any demotion or any other (direct or indirect) discriminatory or retaliatory measure as a consequence of the reporting.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

With the awareness that the employment relationship is imbalanced in favour of the employer, the Italian legislator sought to regulate the scope and the limits of companies' powers, to protect employees from any kind of abuse. In relation to internal investigations, interviews with employees should be conducted carefully to avoid raising disciplinary challenges. Disciplinary proceedings against employees are specifically regulated by the law, requiring the observance of certain formalities, such as a written notice in which the alleged wrongdoings are properly detailed. Challenging a disciplinary violation in relation to interviews may render the subsequent disciplinary proceedings invalid.

There is no distinction for these purposes between officers and directors.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

There are two ways in which an employer can terminate an employment contract: dismissal without notice for just cause (e.g., where there is a serious breach of the employment contract, such as gross misconduct) or ordinary dismissal with notice based on either a subjective reason or an objective reason. In either case, a special disciplinary procedure must be followed. Under this procedure, the employer must promptly send the employee a letter describing the facts that would constitute a breach of the contract, wait for the employee's reply, which must be received within five days, and finally send the employee a letter of dismissal, explaining why the employer cannot accept the employee's justifications.

Suspension, even in the case of misconduct, is not mandatory and does not deprive the employee of salary unless this is expressly provided for by law or by the contract.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

There is no obligation for employees to take part in an internal investigation. However, from a disciplinary standpoint relating to a general duty of co-operation with the employer or specific provisions in a company's policies, a refusal to participate may be relevant. Furthermore, if an employee refuses to participate in such an investigation, the employer may carry out the disciplinary process without the employee's engagement, having first given written notice of this to the employee.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

When an external counsel, appointed for this specific purpose, carries out an investigation, it is important to prepare an investigation plan from the start of the activity. The plan sets out the scope, approach, the issues to be investigated, the investigation team and reporting lines, how legal privilege will be maintained and timing. Measures regarding securing data and necessary steps relating to communication and disclosure might also be outlined in the plan.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There are generally no formal legal obligations on a company to conduct an internal investigation. However, conduct rules issued by regulators may mean an internal investigation is required under those rules, or strongly recommended.

When an issue comes to light, it is strongly recommended to take all necessary steps to stop the offending behaviour, if it is still ongoing, to protect and preserve all material that

would be relevant and to adopt preventive measures to ensure that the offending behaviour cannot occur again.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

This decision depends on the individual circumstances of the case and the nature of the request.

If authorities have issued a binding request, companies should co-operate, in general terms, unless there are indications that the request is not effective or if the privilege against self-incrimination may apply.

In the case of a non-binding request, it has to be decided based on the individual case whether co-operation appears to be advisable. For example, if a specific object is sought by search, the judicial authority may require its delivery. If such objects are handed in, no search shall be performed by the public prosecutor, unless it is believed that the search may be useful for the investigation.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

There is generally no requirement for privately held corporations – with no reporting obligations under the securities laws – to publicly disclose the existence of an internal investigation or contact from law enforcement.

However, listed issuers shall publicly disclose information of a precise nature, which has not been made public, relating to one or more issuers and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments. Therefore, these companies must consider whether the disclosure of an internal investigation or contact from law enforcement would be considered material.

36 How are internal investigations viewed by local enforcement bodies in your country?

There is currently no specific discipline that regulates internal investigations, and it is recommended that companies heed a number of legal issues, such as data protection and employment law-related concerns, as well as the protection of whistleblowers and management of their reports.

Internal investigations could be approached by companies either as a reaction to an investigation started by the Prosecution Service to gather elements useful for the defence as part of criminal proceedings, and to co-operate with the enforcement authorities to discover misconduct and the wrongdoer. Moreover, internal investigations are encouraged to identify and, when possible, prevent the commission of improper behaviour that can trigger liabilities for corporations.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Considering that communications between a company and its in-house lawyers do not attract legal privilege, as recently confirmed by Italian case law, it is advisable that internal investigations are carried out by an external defence counsel, not bound to the client by any employment relationship and appointed for the purpose.

To protect the documentation relating to an internal investigation, it is recommended that it be held at the premises of the lawyer (which cannot be inspected or searched, unless the lawyer is under investigation), labelling any related communications as 'Privileged and Confidential' and restricting the circulation of privileged documents both outside and within the company.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Professional secrecy is usually invoked by the attorney, but in the primary interest of his or her client, who could be either a corporation or a person.

In the case of companies, privilege applies subject to two fundamental conditions:

- the information was exchanged for the purpose of legal assistance; and
- the information was exchanged with an independent, external lawyer who is not bound to the client by any employment relationship and is member of the bar.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

While the attorney–client privilege applies in relation to external counsel, the professional activity of an in-house counsel is neither recognised nor regulated by any legal provision or statute. In-house counsel cannot be admitted to the bar (with some limited exceptions) and are thus deprived of all rights and privileges attaching to independent lawyers who are members of the Italian Bar, including the protection afforded by professional secrecy.

However, some judgments recognise the possibility of invoking the attorney–client privilege when in-house counsel is defending the company in proceedings.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

The law provides for the attorney–client privilege to avoid intrusions that could hinder the defence; therefore, this privilege should certainly extend to foreign lawyers, provided that they are admitted to their national bar and their title is recognised by the Italian system. However, to date, there is no precedent from an Italian court to confirm this reasoning with specific reference to lawyers. There are precedents that have extended the benefit of professional secrecy to foreign private investigators, provided that their title is recognised in the country where the proceedings are pending.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

There is also no general concept of waiving privilege under Italian law.

Public prosecutors consistently state that they cannot expect waiver of the attorney–client privilege and that waiver could not be considered a prerequisite to obtain credit for co-operation. Naturally, submitting privileged documents to authorities is in general regarded as a co-operative step that can result in a reduction of a fine by contributing to a positive overall assessment.

It is mandatory to discuss any initiative with the client. As a matter of fact, divulging a professional secret without justification (or using it for the profit of oneself or a third party), and thereby procuring damage, is an offence.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

As previously said, the Italian legal system does not provide for waiver of privilege (neither general nor limited). However, with reference to criminal proceedings, the jurisprudence has stated that the privilege between a client and an attorney may suffer limitation and restrictions if the lawyer is suspected or accused in criminal proceedings. Even if there is not an actual waiver, in these cases all the information becomes available to third parties, by means of the gathering of that information in the trial dossier.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Waiving privilege in another country has no direct legal effect on privilege claims in Italy. However, waiving privilege in one country by submitting documents to third parties can factually result in a loss of privilege, considering that documents disclosed to non-protected persons may lose privilege.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privilege does not exist in Italy. However, as has already been stated, according to the law, all documents concerning the defence's strategy and all the correspondence between the defending counsel duly appointed and the indicted or investigated person are privileged and cannot be gathered in the trial dossier.

Therefore, in practical terms, the documents and the correspondence in the possession of the attorney that also involves other lawyers and other accused, and which are related to the proceedings and the defence strategy of the client, have to be considered as privileged to protect the client's rights of defence.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

The privilege could be invoked by the attorney even if the defence activity is carried out with the assistance of third parties. Among others, it is possible to include third parties who are trainee lawyers, secretaries, authorised private detectives and technical consultants.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Italian law allows witnesses to be interviewed during an internal investigation. Commonly, this kind of activity is carried out by an external counsel appointed for the specific purpose.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

As stated in question 46, in most cases, it is preferable for the interviewer to be a lawyer, who acts in accordance with all the formalities provided for by the defence investigations provisions of the Italian Code of Criminal Procedure. This ensures that all the findings remain exclusively available to the defence counsel and the client.

However, it should be noted that the privilege does not apply with regard to a company's in-house counsel.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Before the interview starts, the lawyer has to give the interviewee all the warnings provided for by the Italian Code of Criminal Procedure (such as their right to silence or not to give any statement). In addition, there are some rules of deontology that have to be observed (such as informing the witnesses who decide not to give any statements that they could be summoned by the public prosecutor, or before the court during the proceedings, where they also will have to answer the lawyer's questions).

The aforementioned rules apply to employees as well as third parties.

The Italian Workers' Statute provides for specific rules to avoid any kind of abuse from the employer: for example, no permission to investigate an employee's personal views on politics, religion, memberships of trade unions and personal life. Moreover, during an interview, it is necessary to be careful to avoid any disciplinary violation (e.g., a written notice reporting the alleged wrongdoing in detail is required).

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

The Italian Code of Criminal Procedure requires certain formalities to be followed. For example, in the first place, the lawyers give the witnesses a warning (as cited in question 48), then they ask the questions and listen to the answers, all of which is included in a report

(in full of in summary). Finally, the report has to be signed by all the persons attending the interview.

Italian law does not provide for the compulsory presence of the lawyer of the witness during the interview, except when the interviewee is a suspected or accused person in the same proceedings, in joint proceedings or for a joined offence. If that is the case, in order to interview, obtain a statement or gather information, the witness must be accompanied by a lawyer.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Generally, according to Italian law, there is no obligation for a private entity to report crimes to the competent authorities (only public officials have the duty to report what they become aware of within their professional activities). Moreover, a lawyer is not under any obligation to disclose incriminating evidence against a client.

However, there are specific laws that provide for this kind of duty in relation of certain crimes and specific individuals (e.g, the law on anti-money laundering and illicit funding provides for the duty on professionals and intermediaries to report suspected activities).

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

The decision to disclose the findings of an investigation could be encouraged by the positive effect that co-operation with the authorities could have on a judge when quantifying the penalty. Moreover, it can contribute to avoiding the application or determining the reduction of pretrial disqualifying sanctions pursuant to criminal corporate liability law.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

The steps to be taken depend on the specific case at issue and the authority involved, but in any case, there is no obligation to self-report. Moreover, Italian law does not provide for benefits deriving from the disclosure of information gathered through internal investigations. Therefore, from a criminal point of view, it is important to consider in each case whether self-reporting could help in the settlement with the public prosecutor and avoid the application of a disqualifying measure.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

The response will depend on the type of notice received by a company and which authority has sent it. For example, in the case of a request for document production from the public

prosecutor, the company will respond by means of its external legal counsel, which can also arrange an appointment with the authority, through its secretary, to present the documentation collected. Meetings with the public prosecutor can be scheduled, but usually they are accompanied by the filing of a pleading.

54 Are ongoing authority investigations subject to challenge before the courts?

It depends on the kind of investigation.

Generally, a criminal investigation itself cannot be challenged before the courts, but individual measures taken as part of the process (e.g., seizure of documents) can, when unlawful.

The Italian Code of Criminal Procedure provides for the possibility to challenge the request by the public prosecutor to continue with the investigations after the first six-month term has expired.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

In general, it is a requirement to answer all requests received from the authorities. However, in criminal matters, there are now several instruments to strive for mutual co-operation and joint action teams, to prevent unnecessary duplication of effort, from both the private and the public sides.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

If the material is under the control of a company (even by means of a parent company, therefore with a right to take possession, inspect or take copies of a subsidiary's documents), it is required to search and produce all the requested material, even if located in another country.

Nevertheless, it could be that the data protection legislation in the other country does not permit the removal or transfer of the data from that jurisdiction: the requesting authority will therefore seek help from mutual legal assistance with the foreign state.

A parent company could also raise a self-incrimination issue that impedes the delivery of data or documents.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

See question 11.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

During criminal proceedings, the investigations are protected by secrecy, so the public prosecutor and enforcement authorities will not have to disclose information to third parties. However, there are time when investigations are conducted within a mutual assistance regime, in which authorities co-operate and exchange all the data acquired in the respective country.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The advice given will depend on the specific case: in fact, a comparison should be made between the benefits of co-operating with the authority in the company's country and the legal risk of violating a rule in the other country. To achieve this, the company should thoroughly analyse the relevant rules, and request the legal opinion of a lawyer in that country. In cases of gross and evident violation, the best option would be to submit the opinion received to the public prosecutor and encourage a mutual assistance request directly from one authority to the other.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

A request by an authority is usually a sufficient reason for the disclosure of data, according to the Privacy Code, adopted in Italy in 2003, recently modified to be consistent with the GDPR.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Voluntary production can be regarded in a positive light by the judge, as can effective co-operation with the authorities. However, it can generally not be challenged before the courts. In criminal law, even if the investigative dossier is supposed to be protected by secrecy, the company should be conscious that, once a document has been handed to the public prosecutor, it is possible that it will be given to third parties.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Individuals could face financial penalties and detention, or ancillary penalties (such as disqualification).

In respect of vicarious criminal liability, Italian law provides for four types of penalties: financial penalties, disqualifying measures, seizure and publication of the judgment.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

One example of when settlement in another country could be impeded is when there is a disqualification – imposed in Italy – from all activities (which, therefore, includes financial transactions).

64 What do the authorities in your country take into account when fixing penalties?

Italian criminal law provides for specific criteria to fix a penalty.

With regard to individuals, the judge takes into account the seriousness of the crime deriving from several aspects (such as the nature of the offence, the modality of the action, the seriousness of the consequent damage, the intensity of the fraud, existing precedents, the subsequent conduct of the accused, and so on).

Corporations are punished with financial penalties based on a quota system, considering various factors: the seriousness of the deed, the degree of liability of the entity and the activity carried out by the entity to eliminate or diminish the consequences of the unlawful act and to prevent the commission of further unlawful acts. The judge also considers the economic and financial conditions of the entity. The amount of the financial penalty, therefore, is determined by multiplying the first factor (number of quotas) by the second (quota amount). Moreover, if the product or the profit are significant, the sanction could be increased by 10 times the amount of the product or the profit.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Italian case law states that the law on probation is applicable only to individuals, and non-prosecution agreements or deferred prosecution agreements are not provided by Italian law.

It is possible for a corporation to settle a case in advance by means of a special proceeding known as an application of punishment upon request. In particular, the company may agree with the public prosecutor to request the court to impose a penalty (reduced by a maximum of a third), when:

- the employee, whose conduct triggers the corporate liability, settled the case by means of an application of punishment; or
- the only sanction applicable to the corporation is a financial one.

However, the agreement between the company and the public prosecution will be rejected by the judge if he or she feels a permanent disqualifying sanction is warranted.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Non-prosecution agreements or deferred prosecution agreements are not provided by Italian law.

However, proceedings for vicarious liability against a corporate entity are automatically merged with criminal proceedings for an underlying crime allegedly committed by an individual. Therefore, the judicial authority will be aware of the choice of the company in the case of, for example, an application of punishment upon request.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Prior to reaching a settlement with a law enforcement authority, a company should assess the strength of the prosecution and defence cases.

Adverse effects, such as damage to reputation, should be considered. According to Italian law, a settlement cannot be considered a confession of liability by the entity. However, an application of punishment shall be considered equal to a judgment of conviction, unless otherwise provided by the law.

International implications should also be considered, such as the effect the settlement could have in regard to ongoing investigations in other jurisdictions (e.g., whether the authority that has settled will disclose information and assist foreign authorities).

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

External corporate compliance monitors are not used as an enforcement tool. However, in specific cases, the law provides for the appointment of a special commissioner (e.g., when a disqualifying measure should be applied, which results in the interruption of all corporate activities).

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Parallel civil actions are allowed. A civil action brought before the civil court may be transferred to criminal proceedings if, in the civil court, a judgment on merits has not been issued. If the action is brought against the accused in a civil court after joining the criminal proceedings as a civil party, or after a judgment of first instance is issued, civil proceedings shall be suspended until the delivery of a final criminal judgment. The plaintiff may have access to the public prosecutor's dossier.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

According to the Italian Code of Criminal Procedure, investigative acts carried out by a public prosecutor and the police are protected by secrecy, until the accused is entitled to have knowledge of them and, in any case, not beyond the closing of preliminary investigations.

Therefore, publication in the press, or by any other means of communication, of the aforementioned documents or their content, even if partially, is not allowed.

The publication, in whole or in part, of documents that are no longer protected by secrecy is not allowed until preliminary investigations are concluded or the preliminary hearing is terminated. However, if the proceedings reach the trial stage, publication, in whole or in part, of the documents of the investigative dossier is not allowed prior to the delivery of the appeal judgment.

Nevertheless, publication of the content of documents that are no longer protected by secrecy is allowed.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Corporate communication is a delicate aspect of management, which should always be carefully evaluated by experts and approved by the legal office and external legal consultants. In fact, an incorrect press release by a company could have a detrimental effect on customers, and on the strategy eventually chosen during a trial.

The biggest companies in Italy rely on both internal and external professionals for public relations.

72 How is publicity managed when there are ongoing related proceedings?

It is a general rule that the court should not be influenced by press reporting surrounding a trial. Therefore, during criminal proceedings, a company should avoid public communications and, when unavoidable, should make only brief and factual statements that have been approved by their external legal consultants.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Privately owned corporations with no reporting obligations under the securities laws are generally not required to publicly disclose the existence of a settlement.

However, listed issuers shall publicly disclose information of a precise nature, which has not been made public, relating to one or more issuers and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments. Therefore, these companies must consider whether the disclosure of a settlement would be considered material.

Anticipated developments

74 **Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?**

To address corporate misconduct, there is an ongoing debate in Italy in relation to the possibility of making the implementation of 'management and organisational control protocols' mandatory, when requested to exclude corporate vicarious liability.

Moreover, with the adoption of Directive (EU) 2017/1371 on the fight against fraud to the European Union's financial interests (known as the PIF Directive), corporate vicarious liability will be extended to apply to some tax offences.

20

Mexico

Diego Sierra[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Odebrecht is a wide-reaching corruption scandal involving payments in bribes within Brazil, Venezuela, the Dominican Republic, Panama, Angola, Argentina, Ecuador, Peru, Guatemala, Colombia, Mexico, Mozambique and, presumptively, El Salvador and Portugal, totalling US$800 million.

In relation to Mexico, Odebrecht has acknowledged paying US$10.5 million in bribes to officials of the state-owned oil company, Pemex. Mexico has now banned federal institutions and state governments from doing business with Odebrecht SA, a Brazilian construction firm, for the next two years and fined the company close to US$60 million. In addition, the Ministry of Public Function dismissed public official Marco Antonio Sierra Martínez from his position at Pemex, disqualified him from holding any public office for 10 years and fined him US$6.2 million for authorising excess payments for the construction of a Pemex refinery in Tula, Hidalgo.

2 Outline the legal framework for corporate liability in your country.

Corporations can be held liable under administrative, criminal and civil laws.

- Administrative liability of corporations is provided under the General Law of Administrative Responsibilities (GLAR).
- Criminal liability of corporations is provided under the National Code for Criminal Proceedings, the Federal Criminal Code and local criminal codes (depending on the applicable jurisdiction).

1 Diego Sierra is a partner at Von Wobeser y Sierra, SC

- Civil liability of corporations is provided under the Federal Civil Code and local civil codes (depending on the applicable jurisdiction).

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

In terms of administrative liability concerning potentially corrupt conduct, two principal authorities are in charge of imposing administrative liability on corporations: the Ministry of Public Function (which is in charge of investigating improper conducts) and the Federal Court of Administrative Justice (which is in charge of imposing sanctions on corporations). As regards corporate criminal liability, two authorities are involved in imposing liability on corporations, namely prosecutors and courts. Jurisdiction is shared between federal and state authorities for both administrative and criminal liability.

There are no general rules or policies relating to the prosecution of corporations. The guidelines for determining principles of corporate prosecution, the duties of the prosecutors and the factors to be considered for the sanctions imposed would depend entirely on the law enforcement authority applicable to the case.

Jurisdiction between authorities is allocated in federal and state matters, depending on (1) where the conduct took place, (2) the nature of the conduct being investigated, (3) whether there are federal interests involved, and (4) for criminal matters, whether the crime in question is expressly included within the purview of federal jurisdiction as provided under the Organisational Law of the Federal Judicial Power.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Mexican authorities have ample discretion to initiate investigations. However, in practice, authorities will typically start an investigation having been made privy to information suggesting that there are violations to the legal provisions to which the company is subject.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

It would depend on the law enforcement authority involved, and on the remedies provided under the applicable laws. Examples of legal remedies against the lawfulness of a notice are ancillary claims, appeals and *amparo* constitutional review actions.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Yes. Examples of this are as follows:

- An immunity programme, as provided under Article 103 of the Federal Economic Competence Law: any competitor involved in absolute monopolistic practices may file a request with the Federal Economic Competition Commission for an administrative fine reduction, which can be 20 per cent, 30 per cent, 50 per cent or even 100 per cent, depending on the timing of the request as compared with other competitors.

- Opportunity criteria, as provided under Article 256 of the Criminal Proceedings National Code: once an investigation begins, the offender may request that the prosecution authorities refrain from instigating a criminal prosecution (1) when the crime does not have a jail penalty, or has an alternative penalty, or when the jail penalty does not exceed five years, as long as the crime was not committed with violence, (2) in the case of white-collar crimes committed without violence, (3) when the penalty that could be imposed would lack relevance considering another judgment that has already been imposed or could be imposed, and (4) when the accused party provides essential and effective information for the prosecution of a more severe crime than the one attributed to the accused party.
- Criminal liability reduction, as provided under Article 11 of the Federal Criminal Code: a reduction of up to 25 per cent may be granted if a corporation proves that, before the commission of the acts considered as offences under Article 422 of the Criminal Proceedings National Code, it had a compliance department in charge of preventing potential criminal conduct and that it had sought to mitigate the damage caused by the offences.
- Self-reporting, as provided under Articles 88 and 89 of the General Law of Administrative Responsibilities: if a party commits an offence provided therein and self-reports it, the company could request a sanction reduction benefit of between 50 and 70 per cent of the corresponding sanctions provided for the offences committed.

7 What are the top priorities for your country's law enforcement authorities?

The most relevant priorities of the Mexican law enforcement agencies are antitrust, intellectual property, money laundering, fraud, trafficking of minors, environmental matters, corruption and influence peddling.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

There is no specific statute in Mexico regulating cybersecurity. Nevertheless, in June 2018, the Mexican government issued the Official Standards NMX-I-27032-NYCE-2018, NMX-I-27033-1-NYCE-2018 and NMX-I-27032-2-NYCE-2018, providing preventive guidelines to improve cybersecurity controls in Mexico, specifically concerning information security, social media security, internet security and the protection of critical information.

In addition, in late 2017, the Mexican government issued a cybersecurity national strategy to develop a legal regime for cybersecurity, specifically relating to Mexico's economy, national security and public institutions. The aim of the cybersecurity national strategy was to guide all actions incurred by Mexican authorities to prevent, identify, neutralise and mitigate any risks relating to the information contained in data-processing systems.

Since there is no specific statute in Mexico regulating cybersecurity, local law enforcement has been focused mainly on cybercrime.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Cybercrime in Mexico is regulated under Articles 211 *bis* 1 et seq. of the Federal Criminal Code. The person who 'illegally and without authorization modifies, destroys or causes a loss of information contained in private systems or data-processing equipment protected by any security mechanism' has committed a cybercrime. Such conduct may be sanctioned with a prison sentence of between three months and eight years, depending on whether the offender took the information from a private party's equipment, government equipment or a financial institution's equipment, and whether the offender had the authorisation to access the protected data.

Furthermore, as to the approach of law enforcement authorities, the Mexican Federal Police has a special cybercrime unit (cybercrime police) that is responsible for preventing and investigating cybercrimes, and focuses mainly on (1) cyberattacks, (2) the vulnerability of data-processing equipment, (3) data fraud and theft derived from e-commerce, electronic banking services, phishing, pharming, malware and spam, and (4) failure of critical infrastructure. The cybercrime police co-operate directly with private corporations and with authorities from all levels of government, including international agencies such as the Forum of Incident Response and Security Teams, and the Organization of American States.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Criminal law has extraterritorial effects for the purposes of prosecuting foreign bribery in international business transactions. (Mexico will exercise extraterritorial jurisdiction in this context for bribery against both an individual and a corporation.) Article 222 *bis* of the Federal Criminal Code sanctions bribery of a foreign official to obtain an improper advantage.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The principal challenges that arise in cross-border investigations are:

- identifying all laws and policies that may be relevant;
- maintaining confidentiality of what comes to light during interviews with employees. This is often an issue as there is a weak confidentiality culture in Mexico;
- interviewing employees who, in some cases, may have the right to refuse to co-operate and report incriminatory information about themselves and their co-workers;
- implementing controls and efficient processes that take into consideration the cultural differences between countries;
- ensuring effective communication throughout the course of the investigation;
- complying with data privacy and confidentiality laws;
- determining which findings are relevant and which should be reported; and
- determining appropriate remedial actions.

These challenges are compounded when other countries involved have different laws that are applicable to the investigation. Further, remedial action is often determined by both the domestic and the foreign regulators, who have to decide such matters as whether to sanction a company for the violation of a law or to adjust the severity of a criminal penalty that might be assessed against the culprits.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Double jeopardy, or *non bis in idem* defence, is provided under Article 23 of the Mexican Constitution and is understood to mean that no person may be sanctioned twice for the same crime. Hence, if a corporation has faced criminal prosecution and conviction in a country other than Mexico for a certain crime and, thereafter, a Mexican prosecuting authority brings a case against that corporation for the same crime, the corporation could raise this defence. The Mexican Constitution does not limit the defence to crimes relating to the same core set of facts. Moreover, there have been no cases so far that test whether the double jeopardy defence will hold when a corporation has faced prosecution for both administrative and corporate criminal liability relating to the same criminal conduct. However, there have been several cases in the past two years relating to the prosecution of individuals in which the double jeopardy defence is implicated. However, they offer contradictory positions, at times allowing for the imposition of sanctions from both administrative agencies and criminal prosecutors and, at other times, prohibiting parallel sanctions from administrative and criminal authorities. These are non-binding precedent.

There is no 'anti-piling on' policy or analogous provision in Mexico.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not common. However, Mexico has signed international treaties and co-operation agreements with certain countries providing for mutual assistance in criminal, civil and tax matters that may lead to a similar kind of settlement.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

This a relatively new area of law. Mexican authorities may exercise their right to prosecute conduct that is sanctioned under Mexican statute, regardless of whether a foreign authority is investigating the same conduct. Moreover, in the event that Mexico has a multilateral co-operation agreement with the country in which a parallel investigation has already started, Mexican authorities appear to be open to sharing evidence.

One of the most notable examples in recent times is *Odebrecht*, in which Mexican prosecuting authorities have been very vocal in stating that they will not make use of Brazilian agreements to accept evidence collected by Brazilian prosecutors as part of the *Operation Car*

Wash investigation. Mexican criminal enforcement authorities have stated that they are of the opinion that such crimes should be prosecuted under Mexican law to the full extent available. However, they have not made public any details of their investigations. Conversely, on the administrative front, Odebrecht was sanctioned in early September 2018 with a fine of a little over 1 billion pesos (which roughly equates to US$50 million).

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

There is no specific or unified sanctions programme. Instead, Mexico has a fragmented sanctions programme, which is enforced by different law enforcement authorities depending on the type of conduct.

Sanction enforcement in Mexico can be perceived mainly in administrative and criminal instances. In terms of enforcing sanctions for administrative offences:

- the Secretary of Public Function is in charge of investigating the types of corruption regulated under the GLAR; and
- the Federal Court of Administrative Justice is the authority in charge of imposing the corresponding sanctions.

As regards criminal offences, the two main authorities that participate in enforcing sanctions are prosecutors and criminal courts.

The most frequently applied sanctions in Mexico are the following:

- economic fine;
- order to repair damage and lost profits caused to third parties;
- imprisonment;
- debarment from participating in public procurement;
- dismissal of officials, or suspension of employment, commission or position;
- suspension of business activities; and
- dissolution of corporations.

The severity of the sanctions depends strictly on the type of conduct and on the specific circumstances of the case.

A recent enforcement example is the September 2018 sanction imposed by the Ministry of Public Function of almost US$50 million on Odebrecht. The Ministry also debarred Odebrecht and several of its subsidiaries from participating in public procurement processes because of its wide-reaching corruption scandal involving payments in bribes to officials of the state-owned oil company, Pemex.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

In recent months, enforcement on corruption allegations has increased significantly. We can trace this uptick to President Andrés Manuel López Obrador taking office in December 2018 and to the consolidation of certain key enforcement institutions. The Attorney General's

Office (FGR) became independent from the Executive in December 2018. Moreover, the first Anti-corruption Special Prosecutor was appointed in March 2019. López Obrador ran his entire campaign on the promise of eradicating corruption and impunity. It appears his cabinet is taking this seriously.

One example of enforcement recently was the blocking by the Financial Intelligence Unit (which is supported by the Mexican Treasury) of thousands of accounts of people allegedly involved in stealing oil directly from Pemex's pipelines. Further, in the last week of May 2019, the FGR obtained a court order to imprison former Pemex chief executive officer Emilio Lozoya on charges of corruption. There had been news reports since late 2017 linking him to the *Odebrecht* scandal and illegal financing of former President Peña Nieto's 2012 campaign, albeit no action has been brought against him until now.

In August 2019, the former Secretary of Agrarian, Territorial and Urban Development and former Secretary of Social Development in the Peña Nieto administration, Rosario Robles, was sent to prison by a federal judge following accusations of corruption filed against her by the FGR. She is accused of diverting public monies without preventing the squandering of those resources and of failing to report this situation to her direct boss, former President Peña Nieto. The case arose out of a 2018 news report issued by Mexicanos Contra la Corrupción y la Impunidad (a non-governmental organisation) and independent news agency Animal Político, known as the 'Estafa Maestra' (the grand theft), which claimed, in theory, that close to US$350 million of public funds had been corruptly diverted.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Yes, as general rule, Mexican enforcement agencies tend to grant comity to their counterparts in other countries for the purposes of enforcement. Mexico is a party to several mutual legal assistance treaties and thus co-operation tends to be based on those treaties. Moreover, it is typically required that foreign enforcers' petitions comply with at least the following:

- that the foreign authority had the legal competence to impose the sanction pursuant to competence rules analogous to those recognised within Mexican legislation;
- that the offender had been duly notified or served, to assure him or her a fair trial;
- that the object of the procedure from which the judgment derives is not subject to other pending procedures before Mexican courts; and
- that the request to enforce the award is not contrary to public policy.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Mexico has not enacted any specific blocking legislation regarding sanctions measures ordered by third countries.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

There has been no blocking legislation in Mexico.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

It depends on the case, but allegations of misconduct most often come to light by means of:
- due diligence processes (in the context of merger and acquisition transactions);
- internal and external audits;
- whistleblower programmes;
- private complaints or litigation (when filed against a company or its employees); or
- activity reports to a company's appointed directors and officers.

Information gathering

21 Does your country have a data protection regime?

Yes. Articles 6 and 16 of the Mexican Constitution provide for a data protection regime in Mexico. The regulatory laws of this regime are the Federal Law for the Protection of Personal Data Held by Private Parties and the General Law for the Protection of Personal Data Held by Regulated Institutions.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The National Institute of Transparency, Information Access and Protection of Personal Data enforces the data protection regime outlined in question 21. The main objective of the data protection regime is to 'protect the personal data of individuals and companies, with the sole purpose of regulating its legitimate, controlled and informed treatment to secure the privacy and the right of informed self-determination of the people involved'.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

The data protection regime involves the protection of ARCO rights (i.e., the right of access, rectification, cancellation and opposition), which afford an individual the right to:
- access their personal data;
- be made aware of the origin of the data, and executed or anticipated transfers of their data to third parties;
- rectify errors within their data;
- cancel their data when it is held in a manner inconsistent with the law, or when it is no longer needed; and
- to oppose the use of their data by third parties for any type of processing.

Given the technical nature of the collection of data within internal investigations, companies should protect these ARCO rights and be particularly mindful of sensitive data about employees regarding such information as racial origins, ethnicity, health issues and sexual preferences. Privacy notices and consent forms may be required.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

As a general rule, under Article 16 of the Mexican Constitution, all interception of private communications is strictly prohibited. The only exception to this provision applies when a competent authority renders a judicial order providing the legal reasons of its granting, the extent of the intervention, the parties involved and the duration of the intervention. However, this exception shall never apply to electoral, tax, commercial, civil, labour, administrative or attorney–client communications.

In light of the above, to avoid any illegal interception of private communications, companies usually draw up privacy notices and consent forms with their employees, for the purposes of allowing the company to collect, process, transfer and review company documents from the company devices (such as computers, internal and external hard drives, jump or 'thumb' drives, metadata, email, archived email, databases, servers, cell phones, and other cellular and email devices). By means of these mechanisms, employees consent to allow the collection of company-owned data, and employers usually commit to protect employees' personal data. Privacy notices and consent forms are usually prepared in accordance with the requirements set forth in Chapter 1, Articles 3(I), 15, 16, 17 and 18 of the Mexican Federal Law on Protection of Personal Data Held by Private Parties.

Lacking employee consent may expose companies and officials who intercept employees' private communications to criminal liability as provided under Article 177 of the Federal Criminal Code and analogous regulations in the states.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Yes, in relation to criminal matters. Under Article 16 of the Mexican Constitution:

- a judicial authority must order the search warrant;
- the warrant must be limited to a specific place, date and time;
- the object of the search must be strictly specified;
- a probable cause shall be justified; and
- the search must be executed in the presence of two witnesses.

If the aforementioned conditions are not met, all the evidence obtained by the authority by means of the search warrant is inadmissible at trial. Additionally, although there is no automatic redress, a subject company may be able to seek pecuniary penalties from the state and administrative penalties against the authority that exceeded the limits of the search warrant.

Dawn raids are also used by Mexican law enforcement regulators. In recent years, dawn raids have become a particularly invasive feature of antitrust investigations, because there is no injunction available to corporations to effectively defend against the seizure of information by the authorities. In certain cases, the authorities have entered corporations' offices to collect all sorts of data, both electronic and hard copy, for the purposes of their investigations.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

There is no specific protection a party could enforce against the seizure of privileged material before a dawn raid or search warrant is executed. However, there is precedent in the context of antitrust investigations, whereby if the Antitrust Commission collects privileged material in an antitrust investigation, it is obliged to immediately set it apart and exclude it from the investigation. Future cases will have to define the scope of what is covered under this privilege exclusion.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

The Mexican Constitution provides that there is a human right against self-incrimination. Under this right, the defendant cannot be compelled in any criminal case to testify against his or her own interests. This right can be extended to administrative investigations. However, testimony may be compelled from witnesses in possession of facts relevant to the subject matter of an investigation. The general rule is that anyone with knowledge of relevant facts to an investigation being conducted by the authorities has an obligation to testify. The primary exception flows from the privilege that covers what Mexican law calls 'professional secrecy'. This covers professions in which a client has an expectation of privacy from the service provider, such as an attorney, a doctor or a psychologist.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The idea of whistleblower protection programmes is relatively new in Mexico and there are very few legal provisions that incorporate protection programmes. The main example is the 'immunity programme' foreseen in Article 103 of the Federal Economic Competition Law, which provides that any competitor involved in absolute monopolistic practices may make a request to the Federal Economic Competition Commission for a reduction in an administrative fine, which could be as much as 100 per cent, or up to 50 per cent, 30 per cent or 20 per cent depending on the timing of the request as compared with other competitors. If applicable, the Federal Economic Competition Commission will keep the identity of the competitor confidential. In our experience, financial incentive schemes will depend on the applicable statue, the type of conduct, and the subsequent co-operation by the whistleblowers with the law enforcement authorities.

There is no provision for a whistleblower protection programme under either criminal or administrative law.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Under Mexican employment law, there are no specific rights that enable employees to determine how they should be treated during an investigation. However, while conducting an investigation, best practice for an employer should involve:

- providing the employee with a fair opportunity to challenge the allegations being brought against him or her;
- making findings based on objective criteria and evidence; and
- informing the employee of the right to have his or her own counsel and that the interviewing counsel represents the company, not the employee.

Sensitive personal data uncovered during an internal investigation must also be protected. An employer should check the content of its privacy notices regarding the processing of information about employees and ensure that it is consistent with statutory processing conditions.

The officers and directors of a company have the same rights as any other employee. However, 'trusted employees' may be treated differently in that an employer's loss of confidence in a trusted employee is sufficient ground for dismissal of that employee.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

When an employee's alleged misconduct is found to be grounded, the employer may terminate the employment relationship without liability. However, grounds for dismissal follow strict scrutiny and will be interpreted at all times in favour of the employee. Article 517 of the Federal Labour Law provides that an employer has one month to terminate an employee's employment contract or to discipline the employee, starting from the moment the employer becomes aware of the misconduct.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

If an employee refuses to participate in an internal investigation, and the employment contract obliges him or her do so, the employee could be dismissed with cause. However, if an employment contract does not provide that the employee is obliged to co-operate in internal investigations, the employer is unlikely to be able to dismiss the employee for lack of co-operation.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Yes. Such a document would typically include:

- the nature of the investigation;
- the people who will conduct the investigation;
- retention of external support if necessary (external lawyers or external auditors);
- the applicable law during the investigation (data protection, labour rights, criminal, etc.);
- an estimated timeline for the investigation;
- key individuals in the facts under review;
- identification of the databases in which the relevant information may be stored; and
- the individuals who will be subject to interviews or a review of documents.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Pursuant to Article 222 of the Criminal Procedures National Code, 'any individual who is aware of an act that may constitute a crime is compelled to report it to the Public Ministry, or to any police officer if the matter is urgent . . . if any individual fails in this legal duty, he or she will be liable to the corresponding sanctions'. However, the term 'corresponding sanctions' is not defined in the Code. Under the Mexican Constitution, authorities cannot impose penalties if they are not expressly established in law. Article 222 does not provide a specific prison or monetary sanction. Therefore, although companies have a statutory obligation to report facts that may constitute a crime, non-compliance with this obligation will not necessarily carry sanctions.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

- Identify the facts that led to the authority's claim.
- Find and preserve the corresponding data.
- Analyse whether the request for production of documents is valid pursuant to the applicable laws.
- Provide protective measures for sensitive data relating to the company's operations or employees.
- Review the requested data to determine any possible legal consequences.
- Prepare a legal defence regarding any possible legal consequences to which the company might be subject, so as to mitigate risks, when applicable.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

There is no obligation binding a company to publicly disclose the fact that an internal investigation is being carried out, other than Article 105 of the Securities Market Law, which provides that entities registered on the Mexican Stock Exchange must publicly disclose 'relevant events' that may affect the price of their registered stocks.

36 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are a recent trend in Mexico. Mexican enforcement authorities welcome them when they are conducted with a legitimate and serious purpose. Although not required by law, a company can benefit from conducting an internal investigation and co-operating with the enforcement authorities in the prosecution of potential criminal offences or infringements committed by the company's employees or by the company itself. That is to say, an internal investigation can allow a company to prove to the authorities that it has acted diligently and in good faith to try to understand, contain, mitigate and resolve an issue that could potentially result in criminal conduct or an administrative liability.

Further, using the results of an internal investigation, a company can improve its control processes and compliance functions, and implement preventative measures to prevent future infringements. Some law enforcement authorities may even provide 'legal benefits' to a company that has an internal compliance department focusing on the prevention of criminal conduct. For example, Article 11 of the Federal Criminal Code allows for a reduction in criminal liability of up to one-quarter of the penalty provided under Article 422 of the Criminal Procedures National Code (liability of corporations) provided that the corporation can prove that, before the commission of the conduct for which the company is being accused, it had a compliance department in charge of preventing criminal conduct and that, before or after being accused, it sought to mitigate the damage caused by the adduced conduct.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Yes, attorney–client privilege may be claimed over communications exchanged between counsel and his or her client. This criterion has been developed only recently in Mexican law: in an antitrust investigation, the Mexican Supreme Court held that privilege covers communications between a client and its external counsel. In judicial terms, 'communication' is understood to refer to all information exchanged and thus refers to both spoken or written communications (e.g., oral conversations, emails) or work-product (such as written notes, memorandums).

The steps needed for this privilege to attach are that there shall be a contractual relationship between the client and its external counsel, and that there is evidence to prove that the work-product arguably protected is related to the contract between the client and its counsel.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Rather than a specific attorney–client privilege, there is a general obligation for all professionals, including attorneys, to maintain professional secrecy. In the legal profession, this involves both a right to refuse to disclose information about a client, and a duty not to testify, produce documents or disclose any information against a client's interests. Lawyers cannot be compelled to testify against their clients.

The holder of the attorney–client privilege in Mexico is, as a general rule, the client, but sometimes the attorney, depending on the specific case and the interests involved.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

As of January 2017, as consequence of a case dealing with this issue in the realm of antitrust law, the Supreme Court held that the privilege attaches only with regard to external counsel. Principles regarding attorney–client privilege in antitrust law are also incorporated in the technical criteria of 11 December 2018 published by COFECE regarding the management of information derived from legal counsel provided to companies subject to antitrust law.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Yes.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

It is not necessary to waive the attorney–client privilege as part of your co-operation with the authorities. However, counsel has a fiduciary duty towards his or her client to preserve the secrecy behind the privilege.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

No. However, a client may waive the attorney–client privilege if the waiver satisfies the requirements provided under Articles 6 and 7 of the Federal Civil Code that the waiver:

- does not affect public policy or the interests of third parties; and
- is carried out in clear and precise terms, in such a way that leaves no doubt as to the waiving party's intention to waive.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Generally, if the privilege was waived in another country and the waiver was carried out in a manner that fulfils the Mexican law requirements referred to in question 42, the privilege will be considered waived in Mexico as well.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

There is no specific concept of common interest privileges in Mexico. However, there are other recognised privileges under Mexican law, such as banking secrecy and tax secrecy.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Yes. When a third party is providing assistance to a lawyer, there can be an independent privilege of professional secrecy between the lawyer and the third party. If the assistance provided by a third party is connected to the relationship between the lawyer and his or her client, that assistance would also be protected by the attorney–client privilege. Best practice is for external counsel to retain third parties directly and thus secure preservation of this privilege.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes, as there is no legal provision that prohibits such interviews.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Yes, attorney–client privilege will cover an attorney's work-product if the preparation of the work-product was consistent with the attorney's retention agreement and the discharge of his or her fiduciary duties towards the client.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There are no laws setting out particular requirements regarding a witness interview of an employee. However, best practice would include:

- informing the employee that the attorney represents only the company and not the employee individually;
- making the employee aware of the right to have one's own representation;
- explaining the purpose of the interview and the allegations that are being investigated;
- warning the employee that lying or omitting information could constitute illicit conduct; and
- asking the witness if he or she is aware of the company's integrity policies.

Similar requirements apply when interviewing third parties.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

An internal interview will often include the following:
- discussing the background of the interviewee;
- explaining of the nature of the investigation;
- asking the witness about the facts being investigated;
- putting to the witness relevant documents found during the course of the investigation and requesting an explanation from the witness; and
- listening to the witness's clarifications and explanations.

As mentioned in question 48, witnesses have the right to have their own legal representation during the interview. However, no statute or law mandates that the company provides a lawyer for witnesses or employees being interviewed.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

It is mandatory pursuant to Article 222 of the Criminal Procedures National Code. However, as discussed in question 33, there is no sanction for non-compliance with this 'obligation'.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Voluntary reporting may be advisable if failing to report could result in more severe consequences for the company and self-reporting could be used as a defence measure to make a request to the relevant law enforcement authority (national or international) for a reduction in sanctions.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

- Identify the law enforcement authorities to which the company should self-report.
- Identify the legal consequences the company may face after self-reporting.
- Prepare the findings and seek evidence.
- Willingly co-operate with the law enforcement authorities during the course of their investigation.
- Seek penalty reductions for co-operating parties.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Companies may engage in a dialogue with the authorities and opt to co-operate in their investigation to try to seek a reduction of sanctions. Criteria that are taken into account by the authorities are that the co-operating party is the first to co-operate (assuming there are several parties in the investigated scheme), that it provides meaningful evidence to the authorities, that it co-operates continuously with the authorities, and that it suspends its participation in the scheme. Once an authority brings charges against a company, as a general rule, the company may enter into a dialogue to address the authority's concerns.

54 Are ongoing authority investigations subject to challenge before the courts?

Yes. They can be challenged using legal remedies provided by procedural law governing the relevant law enforcement authority (e.g., contentious administrative proceedings or nullity trial) or by constitutional remedies (e.g., constitutional review of *amparo* claims).

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

As a general rule, the best practice will be for companies to seek to negotiate a consistent disclosure package between the various countries issuing notices or subpoenas.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Typically, a company will be required to search for and produce all evidence responsive to the subpoena, even when that evidence is outside Mexico. This issue often arises in investigations relating to bribery of foreign officials, as, although the underlying conduct occurs in other jurisdictions, the conduct is prosecutable in Mexico. Difficulties may arise when responsive evidence exists in a foreign jurisdiction, but production of the evidence in response to the subpoena would violate that jurisdiction's confidentiality laws. However, Mexico has multi-lateral co-operation agreements with several countries that enable authorities to formulate direct requests to obtain evidence that exists abroad.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Yes, Mexico has signed bilateral international treaties under which the parties agree to provide mutual assistance to law enforcement authorities from the signatory countries when requested. Several laws in Mexico include provisions relating to international co-operation; however, the

most relevant laws are the Federal Procedure Civil Code, the Mexican Commerce Code and the Criminal Procedures National Code (for co-operation in criminal matters).

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Yes, under Article 113 of section XI of the General Law of Transparency and Access to Public Information, judicial and administrative files are kept confidential until a final ruling on the matter has been made. Personal information contained in such files are confidential and can never be disclosed.

Furthermore, under Article 106 of the National Criminal Procedure Code, authorities cannot disclose confidential information regarding the personal data of the defendant or any related individual, or share information with third parties. Personal information contained in such files is confidential and can never be disclosed, except to a party involved in the proceedings.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The advice would be to:

- state and demonstrate that the production of such documents would violate the law of the foreign country; or
- state that by producing the documents, the company might be subject to the penalties provided by the foreign law.

Accordingly, it would be 'legally impossible' to perform the object of the request.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

No.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

When a company produces material voluntarily, it has greater latitude to decide what information to give to the authorities. When compelled, the authorities specify the documents and information that have to be provided, and therefore the company can face sanctions if it fails to comply.

As general rule, material – whether produced voluntarily or compelled – is not discoverable by third parties.

With regard to confidentiality, all types of documents and evidence provided to an authority by an individual are confidential and can only be disclosed to the parties involved

in the proceedings. Once the courts enter their corresponding judgments, only the judgment will be published and all private information about the parties (such as their identities) is often redacted. Under Article 70 of the General Law of Transparency and Access to Public Information, all the Mexican law enforcement authorities shall publish 'all resolutions and judgments rendered in processes followed in a manner of trial'. However, Article 73 provides that the law enforcement authorities shall publish 'only the public versions of the judgments that are considered to be of public interest'. Thus, at least in Mexican law, the publication of judgments refers only to the courts' discretion.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Pursuant to Article 422 of the National Code of Criminal Proceedings, the penalties that a company can face for engaging in misconduct include:

- fines;
- confiscation of the instruments used in committing the misconduct;
- disgorgement;
- publication of the judgment;
- suspension of activities;
- dissolution of the company;
- closing down the company's business establishments;
- a ban on any future execution of the types of activities the exercise of which resulted in the misconduct;
- temporary disqualification – for an established period of time – from participating, directly or through a representative, in public contracting procedures such as public bids and government contracts;
- judicial intervention to safeguard the rights of workers or creditors (i.e., the imposition of a government-controlled trustee to remove the company's management so as to halt the alleged crime); and
- public warnings.

Additionally, the directors, officers and employees can be individually responsible for the misconduct and may be punished with a penalty as provided under Article 24 of the Federal Criminal Code, such as:

- imprisonment;
- community service;
- a ban on attending certain places (as determined by the facts of the case);
- fines and fees;
- suspension or deprivation of rights;
- disqualification, dismissal or suspension of functions; or
- a requirement to wear a tracking or surveillance device.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Under Article 81 of the General Law of Administrative Responsibilities, companies that perform unlawful acts (e.g., bribe, influence peddling, use of false information, collusion, misuse of public resources) are subject to the following penalties:

- temporary disqualification from participating in government contracts for a specified period of between three months and 10 years;
- suspension from continuing with business activities for a specified period of between three months and three years; or
- dissolution of the legal entity.

If a company wishes to settle in another country, for that settlement to have effect in Mexico it must be agreed with the Mexican authorities. The General Law of Administrative Responsibilities offers benefits for self-reporting companies, including being spared debarment. Thus, it may be advisable for companies that rely on government contracts to self-disclose and seek leniency from the administrative authorities.

The same principle applies under criminal law. Self-disclosure may bring benefits to the co-operating culpable party provided that it satisfies certain conditions, among which remediation for the damage caused is paramount.

64 What do the authorities in your country take into account when fixing penalties?

Pursuant to Article 410 of the Criminal Procedures National Code, the court shall consider the severity of the crime and the criminal liability of the offender.

The severity of the crime is determined by the value of the legally protected interest, its consequences, the nature of the conduct (wilful or negligent), the means employed, the circumstances of time, mode and place of the event, and the intervention of the defendant.

To determine the criminal liability of the defendant, the court shall consider the circumstances of the event and the wilfulness of the defendant in committing the crime.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Yes, pursuant to Article 256 of the Criminal Procedures National Code, once an investigation begins, the offender can request that the prosecution authorities refrain from instituting a criminal prosecution based on the application of 'opportunity criteria', as long as the damage caused to the victims has been repaired or guaranteed.

These opportunity criteria are only applicable in the situations set forth under Article 256 of the Criminal Procedures National Code, and may apply:

- when the crime is not punishable by imprisonment, when it has an alternative penalty or when the jail penalty does not exceed five years, as long as the crime did not involve the use of violence;
- in the case of white-collar crimes committed without violence;

- if the defendant suffered serious damage as a consequence of the crime;
- if the penalty that could be imposed would lack relevance considering another judgment already imposed or that could be imposed;
- if the accused party provides essential and effective information for the prosecution of a more severe crime than the one attributed to the accused party, and the accused party agrees to testify; or
- if criminal prosecution would be disproportionate or unreasonable considering the causes or circumstances surrounding the commission of the crime.

It is common for the prosecution authorities in Mexico to apply one of the opportunity criteria when it is advantageous to the offender, the victim and the authorities. The possible advantages include (1) fast and effective repair of damage to the victim, (2) no prison penalty, (3) co-operation in the prosecution of more severe crimes, and (4) redress of the damage caused by the crime.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

In Mexican legislation, there are no specific reporting restrictions for corporates that have entered into non-prosecution or deferred prosecution agreements. However, given the nature of non-prosecution and deferred prosecution agreements in Mexico, parties usually agree upon certain conditions for the compliance of the agreement, such as constant co-operation, community service or refraining from certain types of conduct.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Before entering into a settlement with a law enforcement authority, companies should consider:

- the applicable law that would regulate the procedure that allows the application of a settlement agreement;
- the possible legal consequences that the settlement may bring to the company (regarding civil, commercial, criminal and administrative matters);
- the possible legal consequences faced by the company's directors, officers and employees; and
- the extent to which the settlement agreement would mitigate the most risks and consequences for the company.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

It is not common for Mexican law enforcement authorities to use external corporate compliance monitors as enforcement tools.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Yes. Therefore, a defendant may be prosecuted for a criminal act and, at the same time, for a civil claim regarding the same actions.

Private plaintiffs can only gain access to the authorities' files if they are a party to the specific proceeding to which the plaintiffs are seeking access, or if a court requests the authority to produce its files.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Under section XII of Article 113 of the General Law of Transparency and Access to Public Information, criminal investigations undertaken by the public prosecutor are classified. Thus, this information will not be public unless the court discloses it.

Also, Article 5 of the Criminal Procedures National Code provides that all hearings must be public. However, there are exceptions regarding publicity about criminal hearings, such as if the publicity affects the integrity of any of the parties or public security.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

In complex litigation and in situations involving serious crises that affect a company's reputation, it is common practice to retain a public relations firm to manage the situation. Public perception will often have an influence on how the authorities view a case and will guide how they interpret public policy in reaching their decision.

72 How is publicity managed when there are ongoing related proceedings?

Ongoing proceedings are confidential until the issuance of the final judgment (except for personal data, which is generally not disclosed even after a final judgment). Nevertheless, there is often media attention surrounding high-profile cases, particularly with regard to matters of interest to the general public. Sometimes the parties to the proceedings provide information themselves to the media, and even the extent of the conflict itself is publicised. Moreover, it is not uncommon for information about high-profile cases to be leaked to the press and thus become public. Depending on the nature of the case, a party involved in a complex litigation or investigation may attempt to use the media to generate positive public opinion about the merits of its arguments.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

As general rule, there is no obligation to disclose settlements to the market. Article 105 of the Securities Market Law provides that companies registered on the Mexican Stock Exchange

must disclose 'relevant events'. A settlement could be interpreted as a relevant event if, for example, if it could affect the share price.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

On 12 August 2019, the National Law of Asset Forfeiture (NLAF) came into force, replacing all previous laws on the subject. The NLAF regulates asset forfeiture in favour of the Mexican state regarding property with an illicit origin, use or purpose, and the administration and disposal of such property.

Pursuant to the NLAF, property shall only be subject to asset forfeiture if it is related to criminal investigations or criminal proceedings regarding the following:

- corruption;
- concealment;
- crimes perpetrated by public officials;
- organised crime;
- vehicle robbery;
- operations using resources of illicit origin;
- crimes against public health;
- kidnapping;
- extortion;
- human trafficking; and
- crimes relating to hydrocarbons, petroleum products and petrochemicals.

The forfeiting of assets is a civil action – independent of any criminal proceeding – and it will occur in cases where the defendant may not prove legitimate ownership of the assets.

Furthermore, the Ministry of Public Function introduced an integrity programme in late August 2019 to prevent corporate misconduct by establishing mandatory integrity standards among companies in Mexico. The main purposes of this programme are:

- that companies contracting with the Mexican government have principles of probity and integrity certified by competent authorities;
- support and training for companies moving towards a culture of integrity;
- the development of integrity materials and compliance training for Mexican companies;
- the creation of simple materials and content, such as infographics and videos, to ensure that the integrity principles are known and understood at all levels of the company;
- unification of international standards of integrity; and
- the creation of direct reporting channels to the Ministry of Public Function.

According to statements made by the Ministry of Public Function, the law regulating the integrity corporate programme shall be presented to Congress at the beginning of 2020, and compliance with the integrity standards by Mexican companies is expected to be mandatory by 2021.

21

New Zealand

Polly Pope, Kylie Dunn and Emmeline Rushbrook[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

New Zealand's Financial Markets Authority has noted that it has an ongoing investigation into the conduct of CBL Corporation Limited (in liquidation) and its directors. As at mid 2019, the Financial Markets Authority has publicly stated that, following a preliminary assessment, it has concerns about disclosure made as part of the initial public offer, continuous disclosure, financial reporting and directors' duties. New Zealand's Serious Fraud Office publicly announced an investigation into matters relating to CBL in mid 2018.

The High Court appointed liquidators to CBL Insurance Limited in November 2018 on the application of the Reserve Bank of New Zealand, in its capacity as insurance regulator. Further, the Reserve Bank of New Zealand commissioned an independent review of its own supervision of CBL to identify lessons for itself and the insurance regulatory regime.

2 Outline the legal framework for corporate liability in your country.

While there are some offences that on their proper interpretation cannot be committed by corporations (as opposed to natural persons), the general position in New Zealand is that corporations are legal persons and may be held criminally liable for offences. A corporation may be criminally liable for the conduct of employees or agents through the application of the doctrine of vicarious liability, or it may be liable directly or personally.

There is no corporate manslaughter offence under New Zealand law. Although it was considered for inclusion in the Health and Safety at Work Act 2015, it was ultimately excluded.

1 Polly Pope, Kylie Dunn and Emmeline Rushbrook are partners at Russell McVeagh.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The key law enforcement authorities that regulate corporations include the following:

- New Zealand's Serious Fraud Office, which investigates and prosecutes serious or complex financial crime, including bribery and corruption;
- Inland Revenue Department, which is responsible for enforcing New Zealand tax law (including investigating tax-related offending);
- Reserve Bank of New Zealand, which is responsible for enforcing law relating to the regulation of banks, insurers and non-bank deposit takers;
- Financial Markets Authority, which is responsible for enforcing securities, financial reporting and company law relating to capital markets and financial services in New Zealand;
- Commerce Commission, which enforces legislation promoting competition in New Zealand markets and consumer protection legislation, including legislation prohibiting misleading and deceptive conduct in trade; and
- Worksafe, the workplace health and safety regulator, which conducts investigations and criminal prosecutions in relation to workplace health and safety breaches.

Unlike many similar jurisdictions, New Zealand has no centralised agency to take prosecution decisions. Regulatory agencies frequently publish their own enforcement policies. To assist in maintaining a core set of standards for the conduct of public prosecutions, the Solicitor-General publishes Prosecution Guidelines. These Guidelines contain no specific policies relating to the prosecution of corporations.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The statutory requirements differ across enforcement authorities, but in all cases there are limits as to when an investigation can be commenced and information-gathering powers used. For example, the director of New Zealand's Serious Fraud Office requires a reason to suspect that an investigation into the affairs of any person may disclose serious or complex fraud before issuing a notice to produce a document; the director then needs to satisfy the higher threshold requirement of having reasonable grounds to believe that an offence involving serious or complex fraud may have been committed before issuing a notice requiring a person to attend an interview.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Before making any formal challenge, it may be possible to vary the scope and terms of a notice or subpoena through an informal agreement with the issuing authority. A notice or subpoena issued by a public authority may otherwise be formally challenged through an application to the High Court for judicial review.

In a notable example of a challenge through judicial review, notices issued by the Financial Markets Authority requiring the recipients to supply information or produce documents

were declared to be unlawful because of a failure to comply with the statutory requirement to specify a time for compliance.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Most New Zealand regulators' enforcement guidelines provide that proactive and co-operative behaviour should be taken into account when considering enforcement outcome. This is a similar feature in criminal sentencing guidelines.

In the context of competition law, the Commerce Commission operates a specific Cartel Leniency Policy in respect to breaches of the prohibition against cartel conduct. The Cartel Leniency Policy grants immunity to the first person involved in a cartel that the Commission is not aware of, or is aware of but does not have sufficient evidence to launch court proceedings, who reports that cartel to the Commission. Any subsequent cartel members who co-operate will not receive immunity, but may be eligible for the Commission's co-operation policy or the Amnesty Plus scheme.

7 What are the top priorities for your country's law enforcement authorities?

A major focus for New Zealand's Serious Fraud Office has been bribery and corruption, particularly as New Zealand increasingly has links to high-risk jurisdictions, including doing more business with countries in the red zone of the Transparency International index.

The Inland Revenue Department is focusing on implementing proposals to address base erosion and profit shifting, and systems to allow for the greater exchange of information between tax authorities.

Both the Financial Markets Authority and Commerce Commission continue to focus on conduct that has the potential to harm customers, particularly vulnerable customers, or to harm New Zealand's reputation. The Commerce Commission's enforcement priorities for 2019–2020 include environmental claims, online retail, motor vehicle financing and related add-ons, and cartel conduct.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

With the exception of legislation regulating the telecommunications industry, New Zealand does not have any specific laws that impose general obligations on organisations or individuals in relation to cybersecurity. However, the Privacy Act 1993 and the Companies Act 1993 impose certain obligations with cybersecurity implications. The European Union's General Data Protection Regulation may also be applicable to organisations operating in New Zealand where their activities fall within its jurisdiction.

The Privacy Act 1993 requires an agency holding personal information to ensure that the information is protected by reasonable security safeguards against loss, unauthorised access, use, modification or disclosure and other misuse. If it is necessary for information to be given to a person in connection with the provision of a service to the agency, everything reasonably

within the power of the agency must be done to prevent unauthorised use or disclosure of the information.

Under the Companies Act 1993, a director of a company must, when exercising powers or performing duties as a director, exercise the care, diligence and skill of a reasonable director. For most companies, reliance on technology and data is critical to the functioning of business, meaning that this duty of care is likely to extend to the management of cyber risk.

The New Zealand government promotes good cybersecurity practice. CERT NZ is a government agency established in 2017 to receive reports of cyber incidents, analyse threats, share information and advice, coordinate incident responses and be an international point of contact. The National Cyber Security Centre, which is a division of the government's Community Security Bureau, assists New Zealand's most significant public and private sector organisations to protect their information systems from advanced cyber threats. Other regulators, for example, the Financial Markets Authority, also are working with market participants to ensure high standards of cyber resilience and security.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

There are a number of provisions in the Crimes Act 1961 relevant to cybercrime. These sections are very broad and cover (for example) hacking. The offences are treated similarly to conventional crimes in that they fall under the jurisdiction of the New Zealand Police. It is an offence, for example, to:

- dishonestly or by deception access any computer system and:
  - obtain or intend to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or
  - cause loss to another person;
- intentionally or recklessly destroy, damage or alter any computer system where the person knows or ought to know that danger to life is likely to result;
- intentionally or recklessly and without authorisation:
  - damage, delete or otherwise interfere with or impair any data or software in a computer system;
  - cause any of the above to occur; or
  - cause any computer system to fail, or to deny service to any authorised users;
- sell, offer, agree to sell, or possess for the purpose of sale, any software or other information that would enable another person to access a computer system without authorisation where:
  - the defendant knows that the sole or principal use of the software is the commission of an offence; or
  - the defendant promotes the software or information as useful for the commission of an offence, knowing or being reckless as to whether it will be used for that purpose;
- possess any software or other information that would enable the person to access a computer system without authorisation, where the person intends to use that software or information to commit an offence; and
- access a computer system without authorisation (excluding where a person authorised to access a computer system accesses it for a purpose other than the one for which the person was given access).

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Criminal law does not have general extraterritorial effect. However, there is a range of offences relating to conduct occurring outside New Zealand that can amount to an offence in New Zealand. An example is the bribery of foreign public officials by an employee of a company incorporated in New Zealand.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The principal issues that have arisen in the cross-border investigations we have been involved in include:

- ensuring that there is no difference in approach between jurisdiction as to the scope and application of legal advice and litigation privilege;
- ensuring that there is no difference in approach to data protection or privacy laws and that all data transfer arrangements put in place take into account the need to respect these laws and protect legal professional privilege;
- understanding the different legal offences in play across multiple jurisdictions, including determining whether different regimes may have applicable extraterritorial offences;
- ensuring that there is no difference in approach between jurisdictions as to the potential culpability of officers or employees that may result in additional care in respect of providing independent advice to officers or employees;
- ensuring that there are no differences in approach to positive obligations to notify regulators and enforcement agencies of potential offences;
- whether evidence-sharing or mutual assistance treaties exist between the relevant jurisdictions; and
- practical issues around the analysis, review and translation of datasets that include a mixture of languages.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The principle of double jeopardy may apply to prevent a corporation from facing criminal exposure in New Zealand after it resolves charges on the same set of facts in another country. Section 26(2) of the New Zealand Bill of Rights Act 1990 provides that no one who has been finally acquitted or convicted of, or pardoned for, an offence shall be tried or punished for it again. This provision applies to all legal persons, including corporations, by virtue of section 29. Difficult issues could arise, however, and the principle of double jeopardy

could be tested if it is thought that an alleged offender has been unreasonably or improperly acquitted in, or unreasonably leniently punished by, the courts of another country.

New Zealand does not have any laws that are directly analogous to the United States' 'anti-piling on' policy. However, the 'totality principle' in relation to sentencing dictates that, in arriving at the appropriate sentence for several offences, the sentencing judge must not only consider each offence individually, but also assess the offender's overall culpability and determine the effective sentence that is appropriate for the whole of the conduct. The Sentencing Act 2002 provides that, if a court is considering imposing sentences of imprisonment for two or more offences, the individual sentences must reflect the seriousness of each offence. In some circumstances, however, concurrent rather than cumulative sentences may be more appropriate to reflect the gravity of the overall offending.

Specific statutes set out further sentencing rules in particular contexts. For example, the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 provides that, if a person is or may be liable to more than one civil penalty under the Act in respect of the same or substantially the same conduct, civil penalty proceedings may be brought against the person for more than one civil penalty, but the person may not be required to pay more than one civil penalty in respect of the relevant conduct.

13 Are 'global' settlements common in your country? What are the practical considerations?

Such settlements are not common in New Zealand, but there have been examples of information exchange and co-operation between New Zealand authorities and their counterparts in other countries.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

New Zealand law enforcement authorities generally keep abreast of international developments and try to co-operate with their counterparts in foreign jurisdictions. In this respect, New Zealand's Serious Fraud Office, Financial Markets Authority, Inland Revenue Department and Commerce Commission all have standing co-operation agreements in place with equivalent authorities in other jurisdictions.

In the event of a decision by a foreign authority on an identical matter being investigated in New Zealand, we would expect that the New Zealand authorities would take into account that decision but continue to conduct their own investigation.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

New Zealand ratifies United Nations sanctions through regulations promulgated under the United Nations Act 1946. This legislation enables the New Zealand government to act promptly to impose or remove sanctions shortly after a decision has been taken by the United Nationals Security Council. Financial sanctions targeting designated individuals and entities associated with Al Qaeda and the Taliban are implemented separately under the

Terrorism Suppression Act 2002. New Zealand's sanctions are communicated to the public primarily via the *New Zealand Gazette*, the Ministry of Foreign Affairs' website and ministerial press releases.

Outside these existing frameworks, there is no general legislative power to allow the New Zealand government to impose economic sanctions in the absence of a United Nationals Security Council Resolution. Draft legislation that would permit the New Zealand government to impose unilateral or autonomous sanctions in certain circumstances was introduced into the House in May 2017 but has not yet progressed further through the parliamentary process.

Despite not having an autonomous sanctions regime, New Zealand can apply a limited range of diplomatic sanctions in the absence of authorising regulations. These include the refusal of entry visas, the expulsion of diplomats, the suspension of official visits, and the suspension of aid and co-operation.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Sanctions compliance monitoring and enforcement functions are carried out by the New Zealand Customs Service, Ministry of Foreign Affairs and Trade, Immigration New Zealand and New Zealand Police. These government departments have robust systems and procedures in place for monitoring compliance with United Nations trade sanctions, visa restrictions and financial sanctions respectively.

Individuals and companies convicted of an offence under New Zealand's sanctions regulations may be subject to criminal or civil penalties. The maximum penalties are:

- in the case of an individual, imprisonment for a term not exceeding 12 months or a fine not exceeding NZ$10,000; or
- in the case of a company or other corporation, a fine not exceeding NZ$100,000 (per offence).

Evidence of knowledge or intent to breach sanctions will attract significantly harsher enforcement action.

Sanctions enforcement activity has traditionally been limited. New Zealand's first prosecution for a breach of regulations made under the United Nations Act 1946 occurred in 2018. In *New Zealand Customs Service v. Pacific Aerospace Limited* [2018] NZDC 5034, Pacific Aerospace Limited pleaded guilty to three breaches of the United Nations Sanctions (Democratic People's Republic of Korea) Regulations 2006 for supplying a Chinese company with aircraft parts knowing that they would be used to service an aircraft based in North Korea. These breaches carried a maximum penalty of NZ$300,000, but the District Court imposed a penalty of NZ$74,805 owing to a host of mitigating factors.

As a result of this prosecution, New Zealand companies (especially those operating in high-risk jurisdictions) have become increasingly vigilant with respect to their sanctions compliance obligations.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

New Zealand's compliance and enforcement authorities co-operate with their counterparts in other jurisdictions both on a bilateral ad hoc basis, and under the auspices of the United Nations sanctions framework.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

No.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

New Zealand has not enacted any blocking legislation in relation to the sanctions measures of third countries.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct come to light in all manner of ways in New Zealand, including:
- after specific accidents or events that highlight issues;
- through whistleblowers;
- through internal and external audits and compliance reviews;
- through thematic reviews undertaken by regulators; and
- through media reports, including in respect of emerging issues in other jurisdictions.

Information gathering

21 Does your country have a data protection regime?

New Zealand's Privacy Act 1993 governs the collection, storage and disclosure of personal information in New Zealand. The Act applies to all companies and requires that personal information is collected and stored only with an individual's knowledge, and only disclosed with consent, unless specified exceptions are met.

There is currently an amendment Bill before New Zealand's Parliament, which would replace the existing Privacy Act 1993 with a more comprehensive data protection regime that would include a mandatory reporting obligation in the event of privacy breach and would require New Zealand agencies to ensure that personal information disclosed overseas would be subject to acceptable privacy standards.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

Under the current data protection regime, any person may make a complaint to the Privacy Commissioner regarding an alleged breach of the Privacy Act 1993. If the Privacy Commissioner is unable to resolve the matter, proceedings can be brought in the Human Rights Review Tribunal alleging a breach of the Act.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

In our experience, the data protection issues that arise in New Zealand are similar to those encountered in internal investigations in other developed countries.

The Privacy Act 1993 allows disclosure of otherwise private personal information should it be required to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, prosecution and punishment of offences. This can allow the disclosure of personal information to a regulatory agency in the context of an investigation.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Section 216B of the Crimes Act 1961 makes it an offence to intentionally intercept any private communication by means of an interception device. However, it is an exception to this offence if a party has the express or implied consent of the originator or recipient to intercept that communication.

The interception of employee communications that are work-related and using work email or equipment owned by the employer can be lawful, but there are limits to an employer's right to intercept such communications, including privacy implications. Under the Privacy Act 1993, collection of data must be for a lawful purpose and be necessary to achieve that purpose. In addition, an employer should not intrude to an unreasonable extent upon the personal affairs of its employees. An employer should expressly reserve the right to monitor employee emails (and, if applicable, other forms of work-related communications) and make it clear why that monitoring is occurring. The Privacy Commissioner in New Zealand has stated that monitoring of employee work email is acceptable following notification but that the interception of emails from an employee's private email account will not be lawful, even if accessed using an employer's server.

Interception or monitoring of telephone communications may also be lawful in the workplace where there is a good reason for such recordings and employees are aware that they may be recorded.

An employee can raise an issue in relation to interception of communications via a complaint to the Privacy Commissioner or by bringing an employment claim via the Employment Relations Authority.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Authorities that investigate corporate crime in New Zealand, such as the Serious Fraud Office or Financial Markets Authority, may conduct dawn raids of businesses or residential premises under the authority of a search warrant issued by the court or an issuing officer. The Commerce Commission also has similar powers.

The authorities will also consider using their powers to compel companies to provide information via the authorities' respective statutory powers by issuing statutory notices.

When a raid is carried out under a warrant in New Zealand, the authority may use reasonable force to gain entry to the premises. However, it may only search the premises specified in the warrant and seize items within the scope of the warrant. Some authorities have additional powers that can be exercised during the search, including compelling persons to assist with the search or to answer questions relevant to the search, such as how to access electronic documents or where documents are located.

If there are significant errors in the process of obtaining the warrant or authorising the raid, or in its execution, the raid can be challenged by judicial review (in the High Court) and rendered unlawful, and the material seized during the raid could be rendered inadmissible.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

In most instances, legally privileged material cannot be seized during a dawn raid.

The authorities who investigate corporate crime are frequently accompanied during raids by an independent lawyer specifically tasked with reviewing on-site any material that the company asserts as privileged. It is important to be aware of where privileged material is likely to be stored (electronically and physically) so that claims for privilege can be made before items are seized. The company should assert its rights in writing in this regard.

When there is a dispute as to privilege, in practice, the authority will often seal the material or the server (depending on what is permitted to be seized under the warrant) for review by an independent lawyer (typically a barrister) for privilege before it is examined by the investigating team.

Technology such as servers, mobile phones and tablets may contain both privileged and non-privileged material that cannot be separated. These can be seized or cloned during the raid, subject to the terms of the warrant. In practice, the privileged material will then be quarantined by digital forensic experts within the authority and privileged material will be identified by applying search criteria provided by the company.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

An individual providing required information in the course of a proceeding or to a person carrying out a statutory power has a right against self-incrimination when providing testimony. This right does not apply when it is removed by statute, and a number of New Zealand statutes that provide regulatory investigation powers expressly remove this right. Whether information obtained compulsorily is admissible in court will depend on the statute under which that information is acquired.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The Protected Disclosures Act 2000 offers protection to individuals who make qualifying protected disclosures of serious wrongdoing in or by an organisation. A disclosure is protected if the:

- information is about 'serious wrongdoing' as defined in the Protected Disclosures Act;
- individual has a reasonable belief that the information is true (or likely to be true);
- individual wishes to disclose the information for it to be investigated; and
- individual wishes the disclosure to be protected.

A protected disclosure must be made in accordance with the internal procedures of the organisation, unless circumstances permit otherwise.

An individual who makes a protected disclosure is granted three core protections under the Protected Disclosures Act:

- Protection from retaliatory action. The individual cannot be dismissed or disadvantaged in his or her employment as a result of making the disclosure.
- Confidentiality. Anyone to whom the disclosure was made must use his or her best endeavours not to disclose information that might identify the individual (unless the individual's consent is obtained or there is a reasonable belief that disclosure of identity is essential to the investigation or the principles of natural justice).
- Immunity from civil or criminal liability. The individual cannot be sued for making a protected disclosure.

Upon receipt of a protected disclosure, an organisation has 20 working days to take action, and failure to do so entitles an individual to make further disclosure to an appropriate authority.

There are no financial incentive schemes for whistleblowers in New Zealand.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Justification test

Under the Employment Relations Act 2000, an employee may be dismissed or disadvantaged (when in ongoing employment) lawfully only if the employer can justify its action. The test for justification is whether the employer's actions were what a fair and reasonable employer could have done in all the circumstances at the time the action occurred. This is an objective test, which requires an employer's actions to be both substantively justified and procedurally fair.

Characteristics of a fair process in relation to an allegation of misconduct include (but are not limited to):

- conducting a sufficient investigation, having regard to the resources available;
- advising the employee of the nature of the allegations against him or her;
- providing all relevant information and an opportunity to provide feedback;
- providing an opportunity for the employee to be supported by a support person or other representative; and
- genuine consideration of feedback provided by the employee prior to making a decision.

If an employer is unable to justify an action (according to the test above), the employee has a personal grievance. Potential remedies for a successful personal grievance include reinstatement, reimbursement of lost remuneration, and compensation for hurt and humiliation.

Good faith obligation to employees

Both employers and employees owe each other a duty of good faith. This duty includes not doing anything that directly (or indirectly) misleads or deceives (or is likely to mislead or deceive) the other. This also requires parties to be active and constructive in establishing and maintaining a productive employment relationship as well as being responsive and communicative.

Specifically, when an employer proposes to make a decision that will, or is likely to, have an adverse effect on the continuation of employment, the employer has a good faith duty to provide the affected employee with all relevant information. The employer must also provide the employee with the opportunity to comment on the information.

Directors and officers

If a director is also an employee, the above obligations apply with regard to the employment relationship. All directors will also be subject to obligations under the Companies Act 1993, including duties to act in good faith, to act in the best interests of the company and to exercise the care, diligence and skill of a reasonable director in the same circumstances. Failure to comply with such duties may result in additional consequences.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

The employment rights described at question 29 apply to an employee who is the subject of an investigation regardless of whether misconduct is ultimately found to have occurred. If an employee is dismissed as a result of misconduct, the justification test will apply to the employer's actions. Good faith obligations apply for the duration of the employment relationship regardless of the reason for termination.

There is no requirement for an employer to suspend an employee who is implicated or suspected of misconduct. However, suspension may be lawful, provided the employee's employment agreement contains a power to suspend, a dismissible action has been alleged and a fair process is followed.

For a dismissal to be lawful, a full and fair disciplinary process must be followed including (as discussed at question 29) putting the relevant allegations to the employee and seeking the employee's feedback prior to making a decision to dismiss.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

An employee can only be dismissed for refusing to participate in an internal investigation if such a refusal constitutes a failure to follow a lawful and reasonable instruction from the employer. Whether this is the case will depend on whether participation in the investigation is within the scope of the employee's role.

Generally, as discussed at question 29, the justification test and good faith obligations apply to all disciplinary processes or other actions taken by an employer against an employee.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

There is a range of practices in New Zealand depending on the legal representatives engaged. However, it is good practice to draw up written terms of reference. This is particularly the case when an external party is being instructed and there is a desire to ensure a tight rein is kept on the scope of the investigation.

The key purposes of a terms of reference document include:

- setting out very clearly the aims of the investigation;
- defining the scope of the investigation, in terms of both the issues to be covered and any proposed limitations in terms of access to people or documents;
- recording who is conducting the investigation and to whom in the company (and in what form – written or oral) they are to report; and
- setting time frames.

Privilege should be a key consideration when drafting the terms of reference. When litigation privilege may be claimed over a report, the terms of reference should record that the company anticipates proceedings and that the dominant purpose of the investigation is preparing for those proceedings. Given privilege is a matter of substance and not form, this alone will not guarantee a claim of privilege is successful. Further, the terms of reference will also need to be implemented as intended for privilege to attach.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

A company should obtain prompt legal advice on the issue, and should consider matters such as:

- notifying insurers;
- preserving claims against or minimising liabilities to other parties;
- identifying any other jurisdictions and regulators potentially relevant to the issue;
- continuous disclosure obligations;
- any legal obligations to report or regulator policies encouraging self-reporting;
- protecting whistleblowers;
- commencing employment investigations; and
- document preservation.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Upon receipt, the notice or subpoena should be sent to the appropriate person or persons, which will usually include the general counsel. We recommend acknowledging receipt of the notice immediately, indicating that the notice will be considered and that the recipient will revert with any questions or concerns as to the scope or timelines set out in the notice. An initial assessment of the legal basis for the notice (for instance, to check whether it is a voluntary or compulsory request, whether it is validly issued and whether there are any confidentiality obligations) is recommended.

Consideration should then be given to which documents and other materials may respond to the notice or subpoena, and steps should be taken to preserve and hold those documents and materials. Consideration should also be given to how best to address the request, for example keyword searching across date ranges. Issues of privilege, data privacy and (where applicable) bank secrecy and contractual confidentiality obligations should be considered (noting there may be particular issues if a voluntary notice is issued).

Once a plan is developed as to how to respond in terms of process, we typically recommend checking the approach to be adopted with the requestor and explaining any difficulties foreseen in terms of completing what is required within the time frame set in the notice.

The company may be required to take steps to preserve documents and data prior to the receipt of a notice or a subpoena if earlier correspondence with the law enforcement authority suggests a proceeding may be commenced. An obligation to preserve documents exists from the time a court proceeding is reasonably contemplated. Particular consideration should be

given to automated document deletion practices as electronic documents must be preserved in a retrievable format even when they would otherwise be deleted in the ordinary course of business.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Companies publicly listed on the New Zealand Exchange must disclose material information immediately. 'Material information' means information that:

- a reasonable person would expect, if it were generally available to the market, to have a material effect on the price of the issuer's quoted securities; and
- relates to particular securities, a particular issuer or particular issuers, rather than to securities generally, or issuers generally.

Some exceptions to the continuous disclosure obligation apply, notably where information is generated for internal management purposes, or comprises matters of supposition or is insufficiently definite to warrant disclosure. Legal advice is recommended on the application of continuous disclosure rules to a particular internal investigation or contact from law enforcement.

Privately owned companies are not required to publicly disclose the existence of internal investigations or contact from law enforcement.

36 How are internal investigations viewed by local enforcement bodies in your country?

New Zealand regulators and enforcement agencies are typically not opposed to internal investigations that would not impede a criminal investigation. However, if a matter becomes known to an authority before the internal investigation has begun or been concluded, some caution is necessary. At present, New Zealand regulators and enforcement agencies provide less formal guidance on the appropriateness and expectations around internal investigations than in some other jurisdictions.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

In some circumstances, where an investigation is conducted by lawyers and comprises confidential legal advice, or an investigation is conducted for the dominant purpose of preparing for contemplated court proceedings, privilege may be claimed over aspects of the investigation. A company should take legal advice on the applicability of privilege before commencing an internal investigation. Where privilege attaches, the relevant communications or work-product must be kept confidential to preserve privilege.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Under the Evidence Act 2006, legal advice privilege attaches to communications between a person and their legal adviser if:

- the communication was intended to be confidential; and
- it was made in the course of, and for the purpose of the person obtaining professional legal services from the legal adviser, or the legal adviser giving such services to the person.

Corporations can be persons for the purposes of the Evidence Act. The same privilege applies to individuals.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes, so long as the in-house or external counsel holds a current practising certificate. Privilege may attach to communications to or from an in-house lawyer, provided that the in-house lawyer holds a current practising certificate, and provided that the communications were intended to be confidential and were made in the course of, and for the purpose of, the person obtaining professional legal services. Privilege may also apply to lawyers of certain named overseas jurisdictions.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

The provisions in the Evidence Act 2006 pertaining to attorney-client privilege are sufficiently broad to cover advice given by overseas practitioners as defined in that Act.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

The concept of limited waiver of attorney–client privilege is recognised as a potential step, but there are no specific policies or contexts where it is expected by regulators as a matter of course.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The concept of limited waiver is recognised in New Zealand. The Evidence Act 2006 provides that a person who has legal advice or litigation privilege (for instance) may waive that privilege either expressly or impliedly. The Act sets out those situations where privilege will be deemed to be waived generally if the privilege holder:

- (or anyone with the authority of that person) voluntarily produces or discloses, or consents to the production or disclosure of, any significant part of the privileged communication, information, opinion or document in circumstances that are inconsistent with a claim of confidentiality;

- acts so as to put the privileged communication, information, opinion or document at issue in the proceeding; or
- institutes a civil proceeding against a person who is in possession of the privileged communication, information, opinion or document, the effect of which is to put the privileged matter at issue in the proceeding.

In cases of limited waiver, therefore, care needs to be taken, particularly regarding the first bullet point above, by ensuring that confidentiality is maintained over the material.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

The key consideration will be whether the limited waiver in another country is deemed to amount to a general waiver of privilege (applying the statutory test – see question 42).

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

This concept exists in New Zealand and is frequently invoked. The provisions of the Evidence Act 2006 dealing with waiver of privilege (see question 42) will govern whether disclosure of privileged information to a person with a common interest is deemed to be a waiver of privilege. Further, it is key to a successful claim to common interest privilege that disclosure should take place in circumstances of confidentiality.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Communications by clients or lawyers with third parties (such as accountants or other experts) may only attract privilege in exceptional circumstances. Either the communication must be for the dominant purpose of preparing for apprehended litigation, or in certain narrow circumstances the third party may be considered to be the agent of the client for the purpose of communications with the lawyer.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes. However, it is important to remain sensitive both to expectations of any other investigating authority and to employee rights.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Yes, to the extent that any documents fall within the categories of legal advice privilege or litigation privilege, as discussed in questions 32 and 38. This may depend on the context of the investigation, who is conducting the investigation, and any terms of reference under which these persons are engaged.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

When a witness in an investigation is also an employee, an employer's actions must be fair and reasonable in all the circumstances and the employer will owe a duty of good faith to the employee (as outlined in question 29). Unless the interview arises in the context of a disciplinary process against the employee, no additional obligations (including in relation to notification or warning) arise.

The duty of good faith applies only to employees and not third parties (including former employees).

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

The conduct of an internal interview is entirely fact-specific. The employee cannot be misled in relation to the information provided or the questions asked. As a consequence, it is common to put documents to the individual being interviewed. Employees are not required to, but they may have legal representation or a support person present.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

In certain circumstances, it is mandatory to report misconduct to law enforcement authorities in New Zealand. For instance, under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, financial institutions must report certain suspicious transactions. Under the Companies Act 1993, a liquidator must report to the Registrar of Companies certain offences committed by a company or its directors that are 'material to the liquidation'. As another example, under the Financial Markets Conduct Act 2013, a number of parties, including an auditor, issuer, supervisor and manager of schemes established under that Act, must report to the Financial Markets Authority the contravention or possible contravention of an issuer's obligations under that Act, or the likely insolvency of an issuer or a registered scheme.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Relevant considerations for a company in deciding whether to self-report an issue to law enforcement may include the expectations of the relevant agency, whether issues of public health and safety are at risk, and whether agencies in other jurisdictions have been notified.

Like many jurisdictions globally, New Zealand has introduced a leniency policy that provides a cartel participant with immunity from prosecution by the Commerce Commission for its participation in that cartel, as long as that participant is the first party involved in

that cartel to come forward to the Commerce Commission, and meets a number of further criteria (such as ongoing co-operation with the Commerce Commission during an investigation). For cartels that have had global effect or implementation, the decision whether to self-report cartel conduct in New Zealand to the Commerce Commission is often made in coordination with legal counsel in other jurisdictions, as it is often important to know the sequence in which jurisdictions leniency applications are made, and to adopt a consistent approach across jurisdictions.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

The company or the individual should seek legal advice to ascertain its legal risk, and should satisfy itself as to the appropriate strategy. There are some particular considerations in relation to self-reporting under the Commerce Commission's leniency policy. Because full immunity is only available for the first applicant to approach the Commerce Commission, and because the Commerce Commission may decline to offer immunity if it has already begun an investigation of its own accord, time is of the essence.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

New Zealand's transparent approach to government means that agencies are typically open to communication at a range of stages. In practice, companies often enter into dialogue with agencies to clarify the scope of notices and deadlines within which information is requested.

54 Are ongoing authority investigations subject to challenge before the courts?

The exercise of a public power (including, for instance, in an ongoing investigation) may in principle be challenged through an application to the High Court for judicial review.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

In such an event, counsel should liaise closely with the client's counsel based in other jurisdictions, to ensure that any concessions or understandings are aligned. However, it will be important to ensure that any disclosure to a New Zealand agency meets the requirements of the notice in New Zealand and that obligations under New Zealand law (including in relation to data privacy and any confidentiality obligations) are properly considered.

Also the agency in question may have information-sharing arrangements in place with its counterparts in other jurisdictions. For example, the Commerce Commission has entered into a number of international agreements with foreign competition and consumer law protection agencies, which provide for co-operation on matters of common interest. Some

co-operation agreements allow the Commerce Commission to share compulsorily obtained information with overseas regulators even without the party's consent.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

There is often an expectation that a New Zealand company will search for information within its control, even if it is located in another country. However, data protection laws and blocking statutes in other jurisdictions may present legal obstacles to adopting such an approach.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

There are formal mechanisms for New Zealand law enforcement to provide mutual legal assistance to other governments in criminal investigations and prosecutions. Formal mutual legal assistance by the New Zealand government is governed, largely, by the Mutual Assistance in Criminal Matters Act 1992. The New Zealand Police provide informal, police-to-police co-operation to other countries' police forces. In addition, agencies such as New Zealand's Serious Fraud Office and the Commerce Commission have entered into memoranda of understanding enabling the sharing of information with their counterparts in other countries.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

New Zealand agencies such as the Financial Markets Authority, Commerce Commission and Serious Fraud Office are bound by their empowering statutes to maintain a limited standard of confidentiality with respect to information obtained during their investigations. This prohibits publication or disclosure of the information or documents unless the disclosure falls within one of the listed exceptions. Where the party who provided the information consents, or the publication can be justified in light of the purposes of the empowering statute, publication may be permitted.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Generally, a company may wish to consider entering into a dialogue with the relevant New Zealand agency as early as possible to explain that it is prohibited from making the disclosure under the laws of another country.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

New Zealand's data protection laws are primarily set out in the Privacy Act 1993. This sets out 12 data protection principles that apply to both public and private sector entities. These principles are generally similar to those underlying the data protection laws of other developed countries – the Privacy Act was heavily influenced by the Guidelines Governing the Protection of Privacy and Transborder Flows of Data issued by the Organisation for Economic Co-operation and Development in 1980.

A company conducting an investigation will have various obligations in relation to the collection, use, storage, accuracy and disclosure of personal information. Under the Privacy Act, an individual can make a data access request requiring the recipient to provide all personal information held about that individual (subject to limited exceptions).

For the purposes of Article 25(2) of Directive 95/46/EC (the Data Protection Directive), the European Commission has recognised New Zealand as ensuring an adequate level of protection for personal data transferred from the European Union. The effect is that personal data can flow from any of the EU Member States or the three Member States of the European Economic Area to New Zealand without any further safeguard being necessary.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

A company should consider whether providing information voluntarily means (under the particular statute involved) that there is a broader range of circumstances in which the information can be used against it in court proceedings. However, in some contexts, providing information voluntarily will mean that it cannot be shared with overseas regulators without a waiver. There may be circumstances in which compelled production is preferable in light of the risks to the company of breaching confidentiality, bank secrecy or data privacy obligations.

As noted in question 58, New Zealand agencies such as the Financial Markets Authority, Commerce Commission and Serious Fraud Office are bound by their empowering statutes to maintain a limited standard of confidentiality with respect to information obtained during their investigations.

Third parties may make information requests to certain public agencies under the Official Information Act 1982. However, if an investigation is ongoing or the information was provided confidentially, the agency may have grounds, in certain circumstances, to withhold the information.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

The penalties for criminal offences in New Zealand include fines and imprisonment. Multiple corporate regulatory statutes allow agencies to take a range of enforcement actions. Notably, a number of agencies may bring civil proceedings seeking pecuniary penalties against

companies and individuals. In some circumstances, individuals can be debarred from (for instance) being a director or being involved in the management of a company.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

There is no legislative regime for suspension and debarment from government contracts in New Zealand. However, under the Government Rules of Sourcing, a government agency may exclude a supplier from participating in a contract if there is a good reason for exclusion, which includes conviction for a serious crime or offence.

64 What do the authorities in your country take into account when fixing penalties?

Authorities must have regard to binding or relevant sentencing principles when fixing penalties for conviction of a criminal offence. Factors the courts have had regard to include:

- level of culpability;
- harm to victims (investors or the 'nation');
- previous character;
- co-operation or assistance with the investigation; and
- whether a guilty plea was entered and at what stage.

Similar factors have been taken into account in fixing civil pecuniary penalties. In deciding what enforcement action to take, an agency will also be guided by the principles set out in its own enforcement policies.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Some New Zealand agencies (such as the Financial Markets Authority) may obtain 'enforceable undertakings'. An advantage for the company concerned is that they can form part of a settlement and thereby avoid immediate court action. A potential disadvantage is the risk of future breach of the undertaking, as the agency may bring court proceedings for breach of the undertaking itself.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

New Zealand does not have non-prosecution or deferred prosecution agreements. However, in general, the Criminal Procedure Act 2011 provides that a court may grant an order preventing the publication of the identity of any person connected with criminal proceedings or the accused. It may grant such an order if (for example) the publication would be likely to cause undue hardship to the connected person.

Additionally, the Financial Markets Authority and Commerce Commission each have broad powers to make orders prohibiting the publication or communication of any information, document or evidence that is provided or obtained in connection with certain activities of the regulators, including investigations.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Relevant considerations will include the risks of enforcement action if a settlement is not entered into, the nature of the potential enforcement action that may be taken, the strength of the company's potential defence, any reputational risks, whether all relevant agencies are involved in the settlement, whether confidentiality is available, and whether any issues are raised in other jurisdictions as a result of either the settlement or the possible enforcement action.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

The term 'corporate compliance monitor' is not used within the New Zealand regulatory environment. However, regulators may in instances either using their specific statutory powers or in the context of negotiating settlements or enforceable undertakings with parties require independent oversight of a company's compliance programme. For example, section 95 of the Reserve Bank of New Zealand Act 1989 gives the Reserve Bank of New Zealand the power to require a bank to provide a report by a Reserve Bank of New Zealand-approved, independent person. These reviews can investigate such issues as risk management, corporate or financial matters, and operational systems.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Civil claims by private parties running parallel to agency investigations and action are generally possible. The courts may allow a plaintiff in parallel proceedings access to authorities' files. However, particularly where the information sought is of a confidential or commercially sensitive nature, there will often be obstacles to obtaining this information.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

When materials are published in the period leading up to or during a proceeding, the publication of those materials could amount to contempt of court when there is a real risk that it interferes with the administration of justice.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Both communications specialists within the company itself and external public relations consultants are routinely used to manage a corporate crisis in New Zealand.

Generally, the chief executive officer is the company spokesperson and manages messaging in conjunction with the board or with internal communications or public relations teams. In-house and external counsel may also be called on to advise in some circumstances. Some organisations may consult external public relations specialists, particularly if they do not have the expertise in-house, in the face of a crisis.

72 How is publicity managed when there are ongoing related proceedings?

Companies often decline to comment on matters where there are proceedings before the courts. A key consideration tends to be the continuous disclosure obligations of listed issuers of securities.

If information can be disclosed to the public, companies may opt to distinguish between the facts found and the legal consequences. Careful consideration is required, particularly regarding any confidential obligations (such as bank secrecy obligations) when dealing with a voluntary disclosure and whether customer information can be redacted. It may be better for the purposes of public relations to wait until disclosure is required by law.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

There are exceptions to the New Zealand Exchange requirements to disclose material information to the market when information is either confidential or concerns an incomplete negotiation or proposal.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

The New Zealand government is currently considering further regulation in the financial services sector to include new entity-level obligations to ensure that customers are treated fairly throughout an institution's relationships with those customers and a corresponding directors and senior managers regime (potentially akin to the UK Senior Managers Regime or Australian Bank Executive Accountability Regime) to span both prudential and conduct requirements.

In April 2019, the New Zealand government criminalised cartel conduct. From April 2021, individuals who intentionally engage in cartel conduct are liable on conviction to imprisonment for a term not exceeding seven years or a fine not exceeding NZ$500,000 (or both).

22

Nigeria

Babajide Ogundipe and Olatunde Ogundipe[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

No significant new corporate investigations have come into the public domain during the past 12 months. The cases that have received attention in the media have, in the main, tended to be those that came to light more than a year ago, and were reported in the 2018 edition of this chapter. The cases mostly involved Nigeria's petroleum sector and, directly or indirectly, the national oil company – Nigerian National Petroleum Corporation. They included the *Malabu* matter, in which the Federal Republic of Nigeria commenced fresh civil proceedings in the English High Court against JPMorgan Chase and others.

An interesting development, about which few details have emerged, is the announcement, made in July 2019, that the Nigerian Information Technology Development Agency (NITDA) was investigating several entities – from banks, financial technology companies and telecommunication companies, to the National Immigration Service – for alleged breaches of the Nigerian Data Protection Regulation (NDPR), specifically Article 2, which is focused on data retention, protection from theft and unnecessary transfer. The outcome of these investigations will be awaited with great interest as they will provide some indication as to how NITDA will handle breaches of the NDPR.

2 Outline the legal framework for corporate liability in your country.

Many statutes create criminal offences for which corporations may be held liable. Each state of the Nigerian federation has its own criminal laws. In Lagos, the largest state in terms of

1 Babajide Ogundipe is a partner and Olatunde Ogundipe is an investigator/analyst at Sofunde, Osakwe, Ogundipe & Belgore.

population and the size of its economy, the Criminal Law at section 20 makes specific provision for corporate criminal liability. Any act or omission under the Law is attributable to the corporation when 'it is done or omitted to be done by its officer'. In determining which officer's act or omission can be attributed to the company, a court must 'have regard to all the circumstances, including the fact that the person has apparent or real authority to bind the company'. If the prohibited conduct is performed by a person who is not an officer of a corporation, that person will nevertheless be criminally liable if the act or omission was carried out by him or her in the performance of his or her duty as an employee of the corporation and if the corporation failed to take steps to prevent it.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Other than the body charged with the regulation of corporations, the Corporate Affairs Commission (CAC), no specific law enforcement authority regulates corporations. The CAC regulates and supervises companies from incorporation to dissolution. Its functions are listed in the Companies and Allied Matters Act. The CAC can impose penalties and sanctions for corporate misconduct, and for security market-related offences, such as insider trading and market manipulation, most of which are pecuniary in nature.

In addition to the CAC, the Securities and Exchange Commission is charged with the regulation of investments and securities in Nigeria, and its functions are listed in section 8 of the Investments and Securities Act.

The Federal Inland Revenue Service is responsible for the taxation of corporations in Nigeria and may take tax enforcement action against corporations.

The various authorities are created by statute and there is rarely any overlap.

There are a number of other regulatory agencies, such as the Central Bank of Nigeria, which regulates the banking industry, the Department of Petroleum Resources, which regulates the oil and gas industry, and the National Insurance Commission, which regulates the insurance industry.

Other than these, the Nigeria Police Force and the Economic and Financial Crimes Commission (EFCC) also prosecute cases against corporations.

In February 2019, NITDA published the Data Protection Regulation, which empowers approved third-party entities to ensure compliance with the Regulation's terms. The Regulation itself outlines a number of data protection requirements for any data controller, which is defined as any entity that collects data, including employee information, making it extremely widely applicable.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

There are no specified grounds on which law enforcement authorities may initiate investigations. Consequently, it would appear that simple suspicion may be all that is required to trigger an investigation. Usually, however, investigations will only be initiated on the basis of a complaint, or some other written allegation that an offence has been committed, addressed to a law enforcement agency or regulatory authority.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A subpoena may be challenged by making an application to a high court seeking to set it aside. The grounds on which a court will set aside a subpoena include the following:

- the scope of the documents or information requested unfairly burdens or prejudices the recipient of the subpoena;
- there was no factual or lawful basis shown for the issuance of the subpoena; and
- legal privilege, such as attorney–client privilege, spousal privileges and the right against self-incrimination.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

There are no formal rules relating to the granting of immunity or leniency to individuals who assist or co-operate with authorities. However, it is not uncommon for no action to be taken against such individuals.

7 What are the top priorities for your country's law enforcement authorities?

The present Nigerian government, re-elected in March 2019, continues to emphasise that investigating corruption is one of its top priorities. In addition, in recognition of the country's tax base (of a taxable population of between 75 and 100 million people, it has been reported that there are between 10 and 19 million registered taxpayers) and, given the recent decline in the price of crude oil – the country's largest source of income – it has become increasingly important for the collection of tax and customs duties to be more efficient. Nigeria imports a significant amount of goods and there has historically been a significant amount of duty evasion.

The approach by the enforcement authorities continues to be focused more on recovering money than on pursuing transgressors.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

NITDA regulates cybersecurity. All data controllers, as defined by the NDPR, must take security measures, including but not limited to 'protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff'.

However, the NDPR is new and there is no case law yet to show its limits. NITDA has issued draft guidelines that provide for the creation of an Administrative Redress Panel to investigate any breaches of the provisions of the NDPR, which are to be treated as breaches of the National Information Development Agency Act.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

A Cybercrimes Act, passed in 2015, created specific criminal offences in respect of a variety of things, ranging from cyberstalking, the unauthorised access of information and trading in stolen information. It also imposed an obligation on financial institutions to verify the identities of its customers, through documentation, prior to allowing any online transactions. In addition, the statute led to the establishment of the Nigerian Computer Emergency Response Team, which is part of the Office of the National Security Adviser. The body receives reports of cybercrime incidents and issues guidance on cybersecurity best practices. In addition, the EFCC has been known to use the Act in its pursuit of fraudsters. The Act has also been used in the prosecution of persons who have published material that is critical of religious institutions and leaders, and the head of the EFCC.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Nigerian criminal law does not purport to have extraterritorial effect. State and federal criminal laws apply only to persons (natural and legal) within Nigeria.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The principal challenge, and one that has arisen in relation to investigations conducted and concluded outside Nigeria, relates to corporations being pursued, and punished, in Nigeria for conduct that has been penalised outside Nigeria. This occurred, to some extent, to corporations involved in the *Bonny Island* bribery cases. Those corporations were subjected to sanctions imposed by the US Department of Justice and the Securities and Exchange Commission. While from a strictly legal perspective this is not a real problem, as the corporation that is most likely to be subjected to sanctions in Nigeria would probably be Nigerian (foreign corporations are, generally, not permitted to carry on business in Nigeria unless they are locally incorporated), the corporations that were involved did consider action taken against their Nigerian subsidiaries and affiliates as amounting to being penalised for conduct that had already been sanctioned elsewhere.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Under Nigerian law, persons may not be tried for an offence if they can show they have previously been 'convicted or acquitted of the same offence by a competent court' or 'convicted or

acquitted by a competent court on a charge on which he might have been convicted of the offence charged'. However, it is questionable whether this provision would be of assistance to corporations carrying on business in Nigeria, given that foreign corporations wishing to carry on business in Nigeria must incorporate in Nigeria, and be separate and distinct entities from non-Nigerian corporations. A Nigerian corporation would have to have been involved in the foreign proceedings to be able to take advantage of these provisions. Further, since a deferred prosecution agreement does not amount to an acquittal or conviction, this might pose additional challenges to the ability of a corporation to rely on the double jeopardy provisions to avoid being subjected to further action in Nigeria. At this time there is no policy similar to the Policy on Coordination of Corporate Resolution Penalties.

13 Are 'global' settlements common in your country? What are the practical considerations?

Simultaneous resolutions are uncommon. However, companies that have had issues in other jurisdictions have, on occasion, also had to resolve issues relating to the same misconduct separately in Nigeria. Given the possibility that matters in respect of which settlements reached outside Nigeria, where Nigerian authorities also have jurisdiction, may well be pursued, it is always advisable to obtain local advice and, if possible, seek to conclude a resolution of the Nigerian part at the same time as the external settlement.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Much depends on the foreign authority and the corporations involved, and on whatever policy considerations are at play. There appear to be no rules or other objective criteria available to enable an all-embracing answer to this question. On the occasions when foreign authorities have taken decisions in respect of matters that are related to Nigeria, any action taken by Nigerian authorities has tended to be shrouded in secrecy, as the Nigerian authorities tend not to provide information to the public. Consequently, only the authorities and the affected parties (with their advisers) tend to have knowledge of any steps that have been taken.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

We are not aware of Nigeria having any sanctions programme.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Given the absence of any Nigerian sanctions programme, there is no enforcement activity.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Nigeria has no sanctions programme and tends to be the subject of sanctions imposed by foreign governments, rather than the imposer of sanctions.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Nigeria has not enacted any blocking legislation in relation to sanctions imposed on it, or on other countries or individuals.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Nigeria has not enacted any blocking legislation.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct usually surface through whistleblowers, internal audits and media reports. A matter of concern when allegations arise from whistleblowing is the victimisation and dismissal of whistleblowers by corporations.

Information gathering

21 Does your country have a data protection regime?

In February 2019, NITDA turned its Data Protection Guidelines into the NDPR. The document, on its face, claims to be binding on all entities that process data in Nigeria. It limits the power of data controllers to share that data for anything that is not to the benefit of the owner of the data. It also restricts the ability of controllers to transfer data to another country, particularly countries with weaker data protection laws. In addition, certain industries have had data protection regulation from their own regulating bodies. For example, the Nigerian Communications Commission (NCC) requires that all its licensees (telecommunications service providers) take reasonable steps to protect customer information against 'improper or accidental disclosure' and ensure that this information is securely stored. In addition, there is a requirement that information must not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations.

NITDA is the authority responsible for planning, developing and promoting the use of information technology in Nigeria. It is empowered to issue guidelines that may prescribe data protection requirements relating to the collection, storage, processing, management, operation and technical controls for information and, in 2017, it issued draft data protection guidelines. These guidelines, which form the basis of the NDPR, are the only set of regulations that contain any comprehensive provisions relating to the protection, storage, transfer or

treatment of data in Nigeria. Personal data is defined in the draft guidelines as 'any information relating to an identified or identifiable natural person, information relating to an individual, whether it relates to his or her private, professional or public life. This can be anything from a name, an address, a photo, an email address, bank details, posts on social networking websites, medical information or a computer's IP address'. Data controllers are obliged to prevent any transfer of data to any country that does not ensure an adequate level of protection within the prescribed context of the guidelines. The guidelines also recommend that the processing of all data collected shall not take place without the consent of the data subject.

The NDPR also states that NITDA shall create an Administrative Redress Panel to investigate any breach of the provisions of the NDPR. Any such action shall be treated as a breach of the National Information Development Agency Act. The basis for such a provision is unclear as the Act does not confer power on NITDA to create such an offence.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The NDPR outlines an intention to create an Administrative Redress Panel. However, as at July 2019, there has been no further information provided by NITDA about this panel. As the regulations are very new and still in draft form, it is impossible to say how likely enforcement action will be. While it appears that NITDA intends to be very proactive in its enforcement of the Regulation, it remains to be seen how serious it will be about enforcement.

The NDPR outlines fines for non-compliance based on the size of a company: a fine of 10 million naira or 2 per cent of annual gross turnover for the preceding year, whichever is greater, for controllers processing the data of 10,000 subjects, and a fine of 2 million naira or 1 per cent of the gross turnover for the preceding year for controllers processing the data of fewer than 10,000 subjects.

Additionally, the Regulation does not restrict the ability of data subjects to seek redress in a court of competent jurisdiction.

This is all in addition to the existing law based partly on the constitutional guarantee of privacy, which is rather broad, and the NCC's Regulation for Telecommunication Companies.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

In the absence of clear general data protection laws, data protection issues have not been a major cause of concern in the conduct of internal investigations in Nigeria. The introduction of the NDPR has yet to have any noticeable effect on internal investigations, but clearly attention needs to be paid to its provisions. In the past, data protection issues have, generally, not posed any particular problems to internal investigations.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

This has not been directly addressed in the NDPR. However, the Constitution contains the following, somewhat broad, guarantees in respect of private communications: 'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.'

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants and dawn raids are a rarity in Nigeria. When a search warrant is required, it is issued by a magistrate, which is the lowest rank of judicial officer in Nigeria. To obtain a warrant, the law enforcement authority must show that there are reasonable grounds to believe the search will provide evidence that a crime has occurred or is likely to occur, and that evidence relating to this is believed to be in the premises to be searched. Unfortunately, search warrants, and the process for obtaining them, have rarely been subjected to any significant judicial scrutiny. Anecdotal evidence indicates that warrants tend to be issued on request and magistrates do not scrutinise the grounds for them.

In theory, if a law enforcement authority fails to comply with the terms of a warrant, a court may preclude it from using any improperly or illegally obtained evidence in a court proceeding, and may direct the return of such improperly obtained material.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Searches are permitted when law enforcement authorities are able to show that there are reasonable grounds to believe that the search will provide evidence that a crime has occurred or is likely to occur. All material deemed to be connected to the commission of a crime may be seized, whether privileged or otherwise. The relevance of privilege, in relation to seized material, will arise when, and if, a party to proceedings seeks to rely on such material. At that point, the issue as to the admissibility of the material and the weight to be attached to it will need to be addressed by the court before which the question is raised.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

The Evidence Act regulates the competence and compellability of witnesses. Privileges that prevent individuals from providing testimony, which are presently recognised in Nigeria, include attorney–client privilege, spousal privilege and the Constitutional provision preventing a person who is being tried for a criminal offence from being compelled to give evidence at trial.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

There is currently no general law in Nigeria providing protection for whistleblowers. A Whistleblower Protection Bill, first introduced in the National Assembly in 2017, continues

to make its way through the legislature. The Federal Ministry of Finance unveiled a whistleblowing programme in December 2016. Under this, persons providing information relating to the violation of financial regulations, the mismanagement or misappropriation of public funds and assets, theft, solicitation and collection of bribes, procurement frauds and other infractions are entitled to receive rewards, calculated as a percentage of monies recovered, and to do so without their identities being revealed publicly. The Investments and Securities Act provides a framework for the disclosure of information in respect of capital market operators and public companies. In 2011, Nigeria's Securities and Exchange Commission released a Code of Corporate Governance for Public Companies, which includes a provision that all public companies establish a whistleblowing mechanism for the reporting of illegal and unethical behaviour.

The Financial Reporting Council of Nigeria has issued the Nigerian Code of Corporate Governance (enacted in January 2019), which also provides comprehensive guidelines for the protection of whistleblowers in the private sector.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Generally, employees have no specific rights under employment laws that determine how they should be treated if their conduct brings them within the scope of an internal or external investigation. The rights and obligations of an employee are, by and large, regulated by the terms of the employment contract. Similarly, save where there are express provisions creating liability of officers and directors, the rights and obligations of officers and directors are governed by the terms of their contracts with the company.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

When employees are accused of misconduct, employment law does not afford them any specific rights.

The steps an employer may take when an employee is suspected of misconduct depend on the terms of the employment contract. In general, and without specific provisions in the employment contract, corporations may take any number of disciplinary actions against employees suspected of misconduct, including suspension and termination. When an employee is deemed to have engaged in misconduct, upon the conclusion of investigations, the company may dismiss the employee summarily and report the conduct to the appropriate law enforcement authority.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

If such a refusal can be construed as a breach of a contract of employment, for which dismissal would be a lawful sanction, an employee may be dismissed for refusing to participate in an internal investigation.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

As discussed further in question 36, the involvement of external counsel in corporate investigations is not common in Nigeria and, as a result, it is difficult to discern any general practices. However, to conduct an internal investigation properly, there must be some terms of reference, and it would be expected that such a document would include a summary of ascertained facts, the objectives and scope of the investigation, the procedures for the conduct of the investigation and any limitations that there may be in carrying out the investigation.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

When a company becomes aware of issues before the Nigerian authorities, the first step should be to seek local legal advice. There is no positive obligation to ensure that records are secured and retained. However, the destruction or suppression of such records could result in obstruction of justice charges. Similarly, there is no requirement to self-report to regulatory or law enforcement agencies. Any decision as to whether to self-report should be made in each individual case. Currently, it is extremely rare that companies self-report to the authorities. In one instance where a publicly quoted company self-reported issues relating to its accounts, arising from the fraudulent conduct of an individual executive that resulted in the incorrect reporting of stock, all the members of the board were sanctioned and barred from holding office as company directors, including those who had no involvement in the wrongdoing. While the sanctions were eventually overturned, following successful litigation against the regulators, this occurrence reinforces the view that, presently in Nigeria, the best course of action may not involve any self-reporting, given the absence of any reporting framework. It might well be that the best thing to do, once an investigation has been concluded, is to keep the information private and secure and wait to see what action, if any, the relevant regulatory or law enforcement agencies might take.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

As stated in question 33, there is no positive obligation to ensure that records are secured and retained. However, the destruction or suppression of such records could result in obstruction of justice charges. The power to issue subpoenas in Nigeria stems from provisions in civil and criminal procedure legislation. Accordingly, they may only be issued by a court in the context of ongoing proceedings. Consequently, law enforcement agencies and regulatory authorities do not issue subpoenas, as a general rule. Upon the receipt of a properly issued subpoena, the recipient must, in the case of a witness summons, attend the court at the designated time or, in the case of a documents subpoena, attend to produce the documents listed in the subpoena.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Privately owned companies are not required to publicly disclose the existence of internal investigations or contact from law enforcement. However, Rule 187 of the Securities and Exchange Commission's Rules and Regulations, which applies to companies listed on public exchanges, provides: 'All information likely to affect the financial condition of a company shall be made available to the Commission by the company and the Commission shall disclose it on the trading floor immediately the information is made available.'

36 How are internal investigations viewed by local enforcement bodies in your country?

As stated in question 32, internal investigations involving external legal practitioners are rare in Nigeria. When they are conducted, they tend to be in the form of internal and external audits rather than investigations conducted by external counsel. Given their rarity, the authorities do not appear to have any general position on them. There have been instances in which a law enforcement authority has used the product of internal investigations as the basis of a prosecution, in essence merely repeating the process undertaken by the internal investigations to obtain evidence for use in the prosecution.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Attorney–client privilege may only be claimed under Nigerian statutory law when a legal practitioner has been engaged and has received information from his or her client 'in the course of and for the purpose of his employment as such legal practitioner by or on behalf of his client'. Legal practitioners may also not disclose the contents of documents with which they have become acquainted, or the contents of any advice given, in the course, and for the purpose, of their employment as legal practitioners. In addition, the Rules of Professional Conduct for Legal Practitioners impose a duty to keep confidential all communications with clients. There is some doubt as to whether in-house counsel have the same duty, and the issue has yet to be determined in Nigeria. Therefore, to ensure that privilege attaches to an internal investigation, it would be advisable to engage external counsel.

Nigeria is a common law jurisdiction, so it would be open to Nigerian courts to adopt common law privilege rules, as exist in other common law jurisdictions. It does not appear that this issue has been the subject of any reported cases in Nigeria. Therefore the extent to which such common law rules may be accepted in Nigeria remains unclear.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Under the Evidence Act, a legal practitioner may not, except with the consent of the client, disclose 'communications made to him in the course and for the purpose of his employment as such legal practitioner by or on behalf of his client, or to state the contents or condition of any document with which he has become acquainted in the course and for the purpose of his professional employment or to disclose any advice given by him to his client in the course and for the purpose of such employment'. This privilege is the client's and does not extend to communications made in furtherance of illegal purposes.

The Rules of Professional Conduct for Legal Practitioners state the obligations differently, providing that all communications made by a client to a 'lawyer in the normal course of professional employment' are 'privileged'. It goes on to prohibit a lawyer from revealing a 'confidence or secret of his client'. Again, it is clear that the privilege is that of the client. There is no distinction between a client who is an individual and one that is a corporation.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

This is unclear, as there have been no judicial statements on the matter. The answer turns on how in-house counsel are viewed – as employees in general or as lawyers whose client is their employee. As Nigeria is a common law jurisdiction, the views in other common law jurisdictions are relevant. Generally, in-house counsel are lawyers for privilege purposes. Ultimately, the burden of demonstrating that an in-house counsel's communication is privileged falls on the corporation. To establish the privilege, the corporation must show that the in-house counsel's communication:

- was made for the purpose of obtaining or providing legal advice to the corporation;
- involved subject matter within the scope of the employee's responsibilities for the corporation;
- was known by the parties to the communication to be for the purpose of legal advice; and
- was confidential when made and has remained confidential.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

This is unclear. The statutory provisions in the Evidence Act are unlikely to apply to foreign lawyers because the provision relates, specifically, to 'legal practitioners' and that term has been interpreted to refer to persons on the roll of legal practitioners kept in the Supreme Court of Nigeria. Therefore, unless the foreign lawyer is also enrolled as a legal practitioner in Nigeria, the provisions in the Evidence Act cannot apply to such a person. However, to the extent that common law privilege rules are adopted in Nigeria, attorney–client privilege may extend to such advice.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

We are not aware of any instance when this issue has arisen. There are no situations in which the waiver of privilege is mandatory. Generally, the privilege may only be waived by the client – the corporation – but the obligation to maintain client confidentiality is not mandatory:

- when the communication is made in furtherance of any illegal purpose and the acts of the client constitute a crime or fraud or other illegal acts; and
- where permitted by law or to comply with a court order.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

In theory, given the nature and extent of legal privilege, the client may stipulate the extent to which it waives that privilege, and should be able to require parties to which disclosure is made to maintain the confidentiality with regard to further disclosures. However, this issue has not been considered by the courts in Nigeria.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Privilege generally can only be waived with the consent of the client. In relation to attorney–client privilege, no attorney is permitted, unless with the client's express consent, to disclose any communication made to him or her in the course, and for the purpose, of his or her employment. Accordingly, information that is not treated as privileged in another country may still attract privilege in Nigeria, if it constitutes what the law determines to be privileged communication.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

As a common law jurisdiction, Nigeria would recognise common interest privileges, in appropriate circumstances. The privilege would attach to communications between a legal practitioner and other parties who share a common interest with the client, provided those communications are made with a view to developing legal advice in anticipation of, or collecting evidence for, litigation. This privilege also applies to all documents obtained or prepared with a view to litigation.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

When a third party acts under the direction of a legal practitioner, the third party is bound by the same obligations as the legal practitioner.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

The interviewing of witnesses as part of an internal investigation is permitted as there are no laws prohibiting the practice.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Communications made with a view to developing legal advice in anticipation of litigation, or collecting evidence for litigation, is privileged. Therefore, privilege may be claimed when internal witness interviews take place with litigation in contemplation.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There are no legal or ethical requirements or guidance currently stipulated in Nigeria when conducting witness interviews of employees. However, the wise course is to adhere to international best practices.

With regard to third parties, who would have to consent to being interviewed, the situation should be the same as for employees.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

There is no prescribed way to conduct internal interviews. This would be mainly down to the nature of the investigation and any internal company policy and guidelines. Investigations are usually document-heavy so documents will probably be put to the witness if they are relevant to the investigation. Ordinarily, employees do not require their own legal representation; however, there is no law prohibiting it. The only concern for most employees is that the use of legal representation may appear to suggest some measure of guilt on their part.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Under certain legislation, such as the Independent Corrupt Practices Commission Act (reporting the solicitation of bribes) and the Money Laundering (Prohibition) Act, the reporting of certain types of conduct is mandatory.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Generally, we would not advise a company to self-report to any law enforcement agency or regulatory authority. If, as a result of a good relationship with an agency or authority, it were possible to anonymously provide information as to the nature of some infringement and to obtain assurances that the resulting official investigation would not be conducted oppressively, we might advise that a report be made. Otherwise, our routine advice would be not to self-report.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

As indicated in question 51, we would generally not advise self-reporting. However, when self-reporting is contemplated, no information should be passed on to the authorities until attempts have been made to understand how the authority would respond and after assessing that any action that would be taken would not be oppressive or inordinate. Only where there is a high level of confidence would self-reporting be advised.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Law enforcement authorities do not issue subpoenas. They may only be issued by courts in the context of ongoing proceedings.

54 Are ongoing authority investigations subject to challenge before the courts?

The exercise of investigative powers by law enforcement authorities can be challenged by an application to the court if it is considered unlawful. If declared unlawful, the court can order various remedies, such as terminating the exercise of that power or awarding damages. Generally, however, the courts tend not to interfere with the conduct of investigations by law enforcement authorities.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

As indicated in question 53, subpoenas may only be issued by courts in the context of ongoing proceedings. Unless an authority in a foreign country can exercise authority over a Nigerian company, disclosure cannot be enforced against the Nigerian company. Of course, there may be other factors that would influence how a company might react to foreign demands for material. However, there are no data protection laws or blocking statutes in force in Nigeria that would be relevant.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Subpoenas are only issued by courts, and Nigerian courts have no extraterritorial reach, nor do they profess to have. Consequently, if material sought by a properly issued subpoena is not under the control of the company to which the subpoena is addressed, the company is under no obligation to seek to obtain such material and will not be sanctioned for its inability to produce the material.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Information is shared, both formally and informally, with countries with which Nigeria has treaties, conventions or other agreements, and informally with other friendly countries with which the sharing of information is not unlawful.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Any such obligations would depend on how the information is shared. If there is an agreement under which the information is shared, and that agreement stipulates some confidentiality obligations, the Nigerian authorities would most likely abide by them.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

Unless the law enforcement authority in Nigeria may request the production of the documents, we would advise against providing them.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Nigeria has neither blocking statutes nor any general privacy laws, other than the general constitutional right to the privacy of homes, correspondence, telephone conversations and telegraphic communications.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

The primary risk of voluntary production of material is that there are no guarantees as to how the material will be used by the Nigerian authority or agency. The material may also

be subject to disclosure under freedom of information legislation. Although there are no confidentiality rules attached to productions to law enforcement in Nigeria, and Nigerian law enforcement agencies are generally unwilling to share information with non-official bodies, there can be little confidence that such material will not be leaked.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

The penalties applicable to companies are fines and forfeiture of assets. Directors and officers of companies, on the other hand, are subject to imprisonment as well as fines and forfeitures.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Nigeria has no formal framework for suspension or debarment from government contracts, and settlements in other jurisdictions are not usually relevant to the award of contracts in Nigeria.

64 What do the authorities in your country take into account when fixing penalties?

The authorities will consider the gravity of the offence, the punishment prescribed by the law, whether the offender is a first-time offender, any mitigating circumstances and the interest of the public, among other things.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Nigeria has no formal framework of non-prosecution or deferred prosecution agreements.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

The lack of a formal framework for non-prosecution or deferred prosecution agreements means that it is unclear whether or not there would be reporting restrictions or anonymity for corporates that have entered into such agreements.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

The primary considerations would be with regard to whether the settlement needs to be kept confidential and whether it would have any adverse consequences outside Nigeria.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

The Federal Inland Revenue Service and the CAC rely on externally audited financial statements from licensed accountants for publicly listed companies. Additionally, the NDPR issues licences to data protection compliance organisations for the purposes of auditing, training and consulting. The NDPR provides that licensees shall act on behalf of NITDA, which implies that licensees would perform audits, not the NDPR. However, NITDA does not currently require data controllers to engage licensed auditors, therefore it seems that, for the time being, internally produced audits are sufficient for compliance with the Regulation.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Private civil actions can be undertaken at the same time as prosecutions. Private individuals have limited rights to undertake the prosecution of criminal offences. However, Nigeria does not have the concept of complainants being parties to prosecutions undertaken by the state, and complainants have no rights to access the authorities' files.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

There is no law regulating publicity of criminal cases at either the investigatory stage or once the case is before a court. Although persons accused of criminal offences are presumed to be innocent until proven guilty, the absence of jury trials in Nigeria makes it extremely difficult for defendants to contend that pretrial publicity has created a real risk that they will not be afforded a fair trial.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Large companies will frequently use public relations firms to manage crises, but this is rarely made public.

72 How is publicity managed when there are ongoing related proceedings?

If there is public (or media) interest in ongoing proceedings, they will be covered by Nigeria's print and electronic media. Proceedings in court are generally open to the public although they cannot be televised or otherwise broadcast. Documents filed in court are accessible to the public, theoretically, though many courts will place obstacles in the path of persons seeking access to obtain them. For example, judges may direct court registrars to restrict access to court documents to the parties to a legal action. Though there is no legal backing for the restriction of access, there is a lack of understanding among some of the judiciary of the rights of persons to access information under the Freedom of Information Act.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Under the rules of the Securities and Exchange Commission, publicly quoted companies must disclose to the Commission 'all information likely to affect the financial condition' of the company. There is also a requirement to disclose that information 'on the trading floor immediately the information is made available'. Therefore, if a settlement has been agreed with a publicly quoted company and it is 'likely to affect the financial condition' of the company, that must be disclosed to the Commission, which would then disclose it on the floor of the exchange.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

NITDA has been extremely active of late, having made frequent statements relating to the NDPR, and making promises to enforce it. The specifics of this remain to be seen, however. Given the broad range of entities that have obligations under the NDPR, it is likely that there will be a number of developments related to it.

23

Peru

Alberto Rebaza, Augusto Loli, Héctor Gadea, María Haydée Zegarra and Sergio Mattos[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The most relevant criminal investigations relate to *Operation Car Wash*, in which Brazilian construction companies are alleged to have bribed Peruvian public officials to have infrastructure work contracts awarded at inflated prices.

2 Outline the legal framework for corporate liability in your country.

Statute No. 30424 (the law regulating the administrative liability of corporation), in force as of 1 January 2018 and its Regulation, Supreme Decree No. 002-2019-JUS, establish the liability of corporations for collusion crimes, domestic and transnational bribery, influence peddling, money laundering and funding of terrorism. In this sense, if an individual linked to a corporation commits any of these crimes, either in the corporation's name or on behalf of it and to its benefit, whether direct or indirect, the company could be liable for the crime autonomously. However, if the company proves that, before the crime was committed, it had an effective compliance programme in place, it could expect immunity from sanctions or a reduced sanction.

1 Alberto Rebaza is managing partner, Augusto Loli, Héctor Gadea and María Haydée Zegarra are partners and Sergio Mattos is a senior associate at Rebaza, Alcázar & De Las Casas.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Regarding the autonomous liability of corporations foreseen in Statute No. 30424, the investigation will be carried out by a prosecutor, which requires the intervention of the Stock Market Superintendence to issue a technical report regarding the effectiveness of the compliance model of the company being investigated. In the event that the compliance model is not appropriate, the prosecutor could take the company to trial, where a criminal judge could impose sanctions.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The Supreme Court has recently established that to initiate a preliminary investigation, only a 'simple initial suspicion' is required, which in turn constitutes 'the least intensive degree of suspicion'.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

For these cases and others in which the investigated party considers that his or her rights are not being respected, or that he or she is being subjected to illegal requirements (e.g., fishing expeditions), a motion may be filed with the preliminary investigation judge, who may invalidate the subpoena or limit its scope.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Originally, the Code of Criminal Procedure only regulated effective co-operation for natural persons. Depending on the relevance of the information provided, a prosecutor may request a criminal judge to exonerate or reduce the sanction.

Statute No. 30737 (passed on 11 March 2018) modified the Code of Criminal Procedure and now companies are allowed to enter into co-operative agreements with the prosecutor. In exchange for providing relevant, verifiable and timely information to clarify the facts being investigated and to prosecute the natural persons involved, the companies may obtain an exemption or reduction of the sanction.

Likewise, the clemency proceeding established in Legislative Decree No. 1034 (Law of repression of anticompetitive behaviour, passed on 24 June 2008) allows those who violate the competition rules to be exonerated from an administrative sanction or to mitigate its magnitude if they provide evidence that helps to detect and prove the existence of collusion (i.e., a cartel) and to sanction the liable parties.

7 What are the top priorities for your country's law enforcement authorities?

Authorities focus their efforts on the investigation of emblematic corruption or money laundering, which, in some cases, involve the political and business elite. For example, former presidents, political parties that participated in the last presidential campaigns and

construction companies and their directors, among others, are being investigated for the aforementioned crimes.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

The National Cybersecurity Policy of 2017 is applicable to public administration entities. The main aspects of this Policy are (1) to protect the information, data and state information infrastructure and the technology used for processing them from internal or external threats, whether deliberate or accidental, to ensure the confidentiality, integrity, availability, legality and reliability of the information, and (2) to ensure the implementation of legislative proposals and regulations relating to information security or cybersecurity.

Statute No. 30999 (Cyber defence law, passed on 26 August 2019) establishes the regulations framework on cyber defence of Peru, regulating the military operations in and through the cyberspace executed by bodies that are part of the Ministry of Defence within their scope of competence. The purpose of this regulation is to defend and protect the sovereignty, national interests, national critical assets and key resources to maintain the nation's capacity to face threats or attacks in and through cyberspace insofar as they affect national security.

Since it is a very recent law, there is still no case law.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Statute No. 30096 (Law of Computer Crimes, passed on 21 October 2013) sanctions behaviour such as illegal access and attacks on the integrity of computer systems (hacking), propositions with sexual purposes to underage children through technological means, computer fraud, among others.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Article 2 of the Criminal Code establishes a general rule that Peruvian law applies to a crime committed abroad, when:

- the person committing the crime is a Peruvian public official or servant fulfilling the duties of his or her office;
- public security or tranquillity are attacked, or the incident involves money laundering, provided the effects of the incident occur in Peru;
- the act or behaviour offends the Peruvian state and national defence, the powers of the state and the constitutional order, or the monetary order;
- the act or behaviour is committed against a Peruvian or by a Peruvian and the crime is foreseen as susceptible to extradition pursuant to Peruvian law, provided it is also punishable in the state where it was committed and the agent enters Peru in any way; or
- Peru is obliged to repress such behaviour according to international treaties.

In turn, Article 397-A of the Peruvian Criminal Code sanctions those who offer, grant or promote, directly or indirectly, bribery to foreign officials in exchange for obtaining a particular advantage for himself or herself or for others within the framework of international economic or trade activities (transnational bribery).

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

In such investigations, one of the main challenges is the time it takes to process the official communications with the authorities of other countries; for example, for international judicial assistance. However, in respect of the emblematic cases, such as *Operation Car Wash*, the delay in replies and effective assistance by foreign authorities has been considerably reduced.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Under the protection of Article 6(c) of the Code of Criminal Procedure, the *non bis in idem* principle or res judicata is applicable if there is the intention of criminally investigating a company in Peru for deeds that have previously been subjected to a final decision by a foreign authority against the same company.

If a company is being investigated both administratively and criminally for the same deeds and on the same grounds, by virtue of Article III of the Preliminary Title of the Code of Criminal Procedure, the criminal jurisdiction prevails over the administrative one. Other than this, there is no institution that is analogous to the US 'anti-piling on' policy.

13 Are 'global' settlements common in your country? What are the practical considerations?

There is no record any global settlement, neither is there a specific regulation of the matter.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Matters investigated in another country that could have an effect in Peru can be considered as evidence to initiate a criminal investigation. Likewise, the authorities may initiate a judicial co-operation agreement with foreign authorities to share relevant information and evidence. For example, this is happening in *Operation Car Wash* with the information provided by the Brazilian authorities.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

The Peruvian government has not imposed economic sanctions against foreign countries, governments, entities or people who may represent a threat to the interests of Peru or of the international community.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Peru has not applied any economic sanctions.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Not applicable.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

There is no blocking legislation in Peru.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

There is no blocking legislation in Peru.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Misconduct usually arises through media reports, internal audits and, in those companies supervised by the financial intelligence unit (companies within the financial system, mining activity, construction, etc.), through reports of suspicious operations of money laundering to the regulator.

Information gathering

21 Does your country have a data protection regime?

Statute No. 29733 (Law of Personal Data Protection, passed on 2 July 2011) and its Regulation, Supreme Decree No. 003-2013-JUS, have as a purpose to guarantee the fundamental right of protection of privacy. Regarding companies, they are expected to provide appropriate treatment of the personal data of their clients, workers and other natural persons related to their activity.

The titleholder of the personal data has the rights of information, updating, inclusion, correction, suppression, opposition, objective treatment, protection and of being indemnified. The National Authority for the Protection of Personal Data may sanction a company if it proves that it made any inappropriate use of the personal data.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The Peruvian Data Protection Authority has been issuing fines for non-compliance with the rules on personal data protection since 2015. The organisations that have been fined are of different types, including clinics, universities, banks and public entities. As an example, Google Inc was sanctioned in 2016 with a fine of up to 256,750 Peruvian soles.

It is important to bear in mind that Peruvian data privacy rules are applicable not only to natural persons or legal entities established in Peru, but also to those using media located in Peruvian territory.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

In the event that an internal investigation entails sharing information with peers located abroad (for example, a parent company or law firm), the cross-border flow of information must be duly communicated to the national authority and comply with the legal provisions.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Although there is no rule that specifically regulates the control of work tools (email, cell phones, etc.) by an employer, Article 2.10 of the Constitution establishes that every person has the right to secrecy and to the inviolability of communications and private documents.

The Constitutional Tribunal (Docket Nos. 114-2011-PA/TA, 3599-2010-PA/TC and 05532-2014-PA/TC) and the Supreme Court (Cassation No. 14614-2016-LIMA) have established, from a labour point of view, that an employer is forbidden to inspect the use of corporate email assigned to its employees, unless it has the express authorisation of the employees every time the employer wants to log in to view the email. Thus, a general waiver signed by an employee when joining the company will not be sufficient.

However, in the criminal sphere (Nullity Appeal No. 817-2016/Lima), the Supreme Court established that if there is a high probability that corporate email has been used to exchange communications with criminal content, it is not illegal or unconstitutional for the employer to inspect its employees' email for the purposes of a criminal claim. A prosecutor may subsequently use the email as admissible evidence in a criminal procedure.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants are used frequently by Prosecutors, particularly in emblematic investigations for corruption or money laundering crimes, such as *Operation Car Wash*.

According to Article 214° of the Code of Criminal Procedure, a search can be carried out when there are reasonable reasons to consider that evidence may be found inside the premises subject to the search. Authorisation by a judge is required.

Both the search and the seizure of documents must be limited to what has been authorised by the judge. There is a possibility of controlling a warrant dictated by a judge through an appeal in which the pertinence, proportionality and reasonableness of the measure are discussed. However, even if the search is considered legal, the judge can be asked to exclude privileged material and any documents not related to the investigation.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Privileged material cannot be seized during a search ordered by a judge and carried by a prosecutor. In this sense, it is recommended that all materials or reports of this nature be labelled as 'protected under professional secrecy', in accordance with the procedure established in Article 2.18° of the Constitution, Article 30° of the Attorney's Code of Ethics and Article 165° of the Criminal Code. Moreover, the presence of an external lawyer is recommended during a search to enforce privilege over documents having such a condition. The Supreme Court has ruled that 'the right to the professional secrecy must prevail over the right to obtain evidence' (Cassation No. 272-2016-Tacna, fj. 13).

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

As investigated parties, people are not compelled to testify. They have the right to remain silent, and silence cannot be treated negatively. As witnesses, however, people are compelled to testify. Nevertheless, there is the possibility of opposing the testimony when some specific circumstances apply, such as the fact that questions may refer to the witness's own criminal liability, that the investigated party is a close relative or that the questioning is about some type of professional secrecy or state secret.

Moreover, investigated parties are not compelled to collaborate with their own prosecution.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

There are no specific financial incentives for whistleblowers in criminal procedures. However, Article 39° of the Regulation of Statute No. 30424 establishes that companies must adopt protection measures to avoid retaliation against the people that use a whistleblowing channel.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

During the process of an internal investigation, 'non-specific labour rights' are applicable. This relates to actions, the legal entitlement – and enforceability – of which goes beyond the standard entitlements of workers (as set forth in the Constitution), such as presumption of innocence, due process, right of defence, right to intimacy, right to secrecy and inviolability of communications, among others.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

All employees have the same rights during the term of the work contract. During an investigation, the employer cannot adopt any type of preventive measure (for example, suspension of the contract), unless he or she has the employee's consent. The only exception to this rule is foreseen for cases of sexual harassment, in which the employer is entitled to suspend – or transfer to another workplace – the alleged harasser to protect the victim.

Without prejudice to the foregoing, in practice employers usually grant paid leave unilaterally to the employees involved in an investigation. Notwithstanding, this practice could be questioned alleging an affectation to the right to 'effective occupation'.

Finally, the employer may adopt disciplinary measures when he or she indubitably verifies that an employee has engaged in labour misconduct or irregularity. In the event a dismissal proceeding is initiated, the employee must be notified in a letter detailing the facts that constitute the serious offence that may lead to his or her dismissal.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

As a general rule, an employee's participation in an investigation should be voluntary or consented.

However, the seriousness of the investigated deeds and their relation to the position of the employee could mean a failure to comply with the labour obligations in the event that he or she refused to collaborate during an investigation process. In such a situation, we consider that this would constitute an assumption of violation of the labour good faith. In

this situation, the employer may impose reasonable and proportionate disciplinary measures (warnings, suspensions or even dismissal).

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is not a common practice. However, it is recommended that at the commencement of each internal investigation, a document be prepared defining its objectives and scope. Likewise, among other aspects to prioritise, the hypothesis of the investigation, the team in charge of the investigation and the means of proof to be used should be defined, as well as the fact that, owing to the nature or complexity of the investigated deeds, external advice will be required, both legal and regarding public relations.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There is no legal obligation for companies to report dishonest behaviour that has occurred. However, once an internal investigation has commenced, the company must try to remedy or compensate the damage caused, identify and correct any internal proceeding the failure of which originated the dishonest behaviour, particularly any action relating to the compliance model. Likewise, according to Article 38° of the Regulation of Statute No. 30424, the internal investigation and subsequent self-reporting could be taken as a sign of an effective compliance model and, therefore, could release the company from liability.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

It is advisable for the company to have a protocol to address such requests satisfactorily and in which the following steps are established:

- Identification of the actions that have brought about the authority's request, in collaboration with the company's legal department or external legal advisers.
- Verification of the validity of the authority's request, that is to say it is not violating any fundamental right such as due process, professional secrecy or protection of personal data.
- Informing the competent authority if the information is in the hands of third parties or if it requires a third party's authorisation to be submitted.
- A detailed review of the information, prior to submission, to identify any legal contingency that could arise from it.
- Designing a defence strategy, both from a legal and a communication point of view, to mitigate the contingencies that could be generated by the submission of information.
- If, as a result of receiving a notice or subpoena, a company becomes aware of any dishonest behaviour within the company, an internal investigation must be commenced to establish its scope.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

There is no obligation to publicly disclose the existence of an internal investigation. However, at the moment of deciding whether to disclose this information, companies must take into consideration the following factors:

- the degree of probability that the prosecutor or another authority becomes aware of the facts that are the subject matter of the investigation;
- the existence of an internal investigation may demonstrate to the authorities that the company itself, through its compliance model, identified, investigated and sanctioned dishonest behaviour; and
- by collaborating with the authorities in providing relevant information that allows clarification of the criminal deed, the company could be applying for an attenuation or exemption of the sanction.

36 How are internal investigations viewed by local enforcement bodies in your country?

Spontaneous internal investigation for suspicion of criminal wrongdoings is a tool that has only recently been available within the Peruvian corporate environment. There is still no case law about its real worth to the authorities. However, any form, or sign, of collaboration with the investigation is always well received by prosecutors.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Although there is no specific regulation in Peru, the attorney–client privilege could be claimed over the findings of an internal investigation in which an external attorney directly participated. In this sense, it is advisable that the instrument or document that initiates the investigation identifies the external attorneys who will participate and that their intervention is documented, for example, during the interviews and in the communications exchanged by the team in charge of the inquiry.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

According to the Code of Ethics of the Peruvian Bar Association, there is no distinction in the treatment of the attorney with the client when the latter is a natural person or corporation. In this sense, the scope of the attorney–client privilege is the same for both.

Likewise, in the framework of an internal investigation, to avoid the lawfulness of the gathered information or the scope of the attorney–client privilege being questioned, it is advisable to inform the parties at each stage of the investigation that the external attorney

only represents the interests of the company; thus, the privilege will be between the attorney and the company and not between the attorney and the employee being interviewed.

The holder of the privilege is the client.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Although there is no specific regulation in Peru, based on the guidelines adopted by foreign courts (for example, in the European Court of Justice *Akzo Nobel Chemicals Ltd* case), a sector of Peruvian specialists considers that the attorney–client privilege only applies when external attorneys are involved.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

To the extent that the waiver to the privilege corresponds to the client, it would apply equally to the advice provided by both national and foreign external attorneys regarding an investigation carried out in Peru.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

In the framework of an effective collaboration, if a company wants to obtain a benefit that, in the best-case scenario, exempts it from liability, it is advisable to waive the attorney–client privilege, if necessary, to provide all the information required by the authorities. Waiver of this privilege is always voluntary.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

There is no specific regulation in Peru. However, a company could waive privilege before the prosecutor and maintain privilege before third parties denying the production of the same information. However, law enforcement may share the information waived to other government agencies.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

The attorney–client privilege can be maintained in Peru after a limited waiver in another country. However, the information disclosed in another country may be shared with Peruvian authorities through international co-operation.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

This concept does exist in Peru. If there are no conflicts of interest, the same attorney may represent several clients in the same criminal procedure.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

The attorney–client privilege extends to those who assist external attorneys, such as experts, accountants and translators, among others.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Yes (see also question 39). In turn, it is advisable that at each stage of an internal investigation, the external attorney announces that his or her intervention is on behalf of the company and not as an attorney of any internal witness.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

The parameters of the interviews within an internal investigation are not regulated in Peru. However, to avoid the admissibility of the gathered evidence being questioned in the event the company decides to share it with the competent authority, it is advisable to inform the employee or third party before starting the interview that the attorney–client privilege applies to the company and not the employee or third party.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Although there is no predetermined protocol for conducting interviews, it is common that an attorney participates in them as a representative of the company. Likewise, minutes are usually written, transcribing part of the information provided. This document is signed by the interviewed employee as a declaration that it conforms with what was said.

It is not common that employees have their own legal representation during interviews. However, if an employee does request the attendance of a lawyer, the employer should agree to the request to prevent the employee from alleging any coercion in making his or her statement.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

There is no legal obligation for companies to report misconduct to the authorities.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting is advisable when it is probable that the company may obtain a benefit in exchange for the information it provides and that the prosecutor may find out about the wrongdoing by other means. Self-reporting will be considered as evidence that the compliance programme of the company was efficient and the company could receive a reduced penalty or even an exemption from a penalty. If the decision to self-report has been made in Peru, it is advisable also to make the self-report in other countries that have jurisdiction to prosecute the crimes.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

There is no express regulation on how to self-report. It is advisable that an external attorney seeks an interview with the prosecutor order to establish his or her interest in the matter. However, it is also advisable to delay arranging such an interview until after an internal investigation has established the actual scope of the misconduct, the persons involved and the legal, financial and reputational contingencies that could be activated.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

How a company should respond to a notice or subpoena will depend on the conditions under which it has been served. If the company is included as a defendant in an investigation, it is recommended that its attorneys review the case file held by the authorities before providing any kind of statement or information. However, if a company has been called only as a witness, its lawyers do not have the right to review the case file. Nevertheless, the company representative who has been called as a witness does have the constitutional right to be advised by an attorney during his or her testimony before the authorities.

In-house or external lawyers may have interviews with prosecutors to address their concerns, such as to clarify the scope of the subpoena and the deadline to comply with.

54 Are ongoing authority investigations subject to challenge before the courts?

Motions challenging investigations may be filed when the investigated deeds lack any criminal nature or when fundamental rights are violated, such as due process, the right to produce evidence, etc.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Companies should address the local subpoena to the full extent regardless of the existence of a foreign subpoena. Local law enforcement authorities will not take into account the subpoenas issued by foreign authorities in making any alterations to the scope of their inquiry and will expect compliance with the local request. Therefore, companies should verify that the information provided to the different authorities, both domestic and foreign, is not contradictory.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

The general rule is that the company must comply with the subpoena. However, if the scope is unreasonable or the costs to produce the material are prohibitive, a motion may be filed to the competent judge (see question 5).

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Lately there has been an increase in law enforcement co-operation with other countries as a result of *Operation Car Wash*. The Code of Criminal Procedure regulates the formalities that must be observed.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

A prosecutor's investigation is confidential. Only the investigated parties and the attorneys of the alleged victims may have access to it (note that in corruption or money laundering cases, the victim is represented by the state attorney). If the case reaches trial, which is public, the information may be disclosed.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

A legal report from counsel in the foreign country should be obtained, explaining that the information may not be produced.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

There are some sectors in which statutes of secrecy exist, such as banking, tax reports and communications. In the event that a foreign state requires this type of information, it must obtain an order from a Peruvian judge.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

The confidentiality of the information or documentation provided to the authorities need only be maintained during the investigation phase. The information may be revealed at trial. Further, foreign regulators may seek the information produced through international co-operation channels.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

The sanctions to companies imposed by a criminal judge are fines, temporary suspension of activities, cancellation of licences, debarments and, when they have been incorporated and operated just to commit crimes, the dissolution of the company. A monitor can be appointed for up to two years. The natural persons, public and private officers can be sanctioned with imprisonment, fines and disgorgement. All this without prejudice to repairing the generated damages that must be jointly and severally assumed by the natural persons and the company.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Peruvian courts have no jurisdiction to avoid companies resettling in another country. However, information about local wrongdoing may be shared to foreign authorities through international co-operation to enable suspensions or debarments.

64 What do the authorities in your country take into account when fixing penalties?

A judge will take into account the benefit the company has obtained or expects to obtain from committing the crime when imposing a fine, which is usually between twice and six times the amount of the benefit. If the benefit cannot be determined, the company's annual income will be taken into account by the judge to fix the fine.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Yes. For this purpose, the company must admit committing the crime, provide evidence against third parties – usually public officers – and remediate. In exchange, the companies could obtain exonerations or reduced sanctions. If it is found that the companies hid information or did not fully collaborate, the agreement can be reverted and the criminal proceedings may continue.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

The effective collaboration agreements are ruled precisely by secrecy from the beginning to the end of the investigation. The other investigated parties do not know the identity of the collaborator.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

The company should weigh the collateral effects of confessing to committing a crime, such as reputational and financial damage. Likewise, the company should take into account that its collaboration may result in members or former members of the company being sentenced to imprisonment.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Since January 2018, external monitors may be imposed for up to two years as a sanction by a judge. However, such a measure has not been enforced to date.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Private actions parallel to the criminal proceeding are allowed, as is a proceeding for reparation or indemnification for damages. However, if the injured party so desires it, that party can take on a civil action in the criminal proceeding and request civil reparation in the same criminal proceeding. In these circumstances, the party injured by the crime will have access to all the evidence in the criminal proceeding.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

The Code of Criminal Procedure establishes the prohibition of publishing the procedural actions during a prosecution investigation. However, the trial is public. There are certain exceptions, including when the sexual morality, the private life or the physical integrity of someone participating in the trial is affected, when national security is affected, or when a particular commercial or industrial secret is threatened.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

There is no general rule, and our recommendations will vary depending on the assessment of each case. Having said that, if the client is a large corporation and is facing a severe crisis

related to a criminal investigation, we always advise hiring a public relations agency, which should work alongside the lawyers to assess both the accuracy and the strategic effects of the information provided to stakeholders and of public opinion. Further, the company's strategy should aim to stop the spread of news relating to any criminal contingency.

72 How is publicity managed when there are ongoing related proceedings?

Publicity depends on the degree of media coverage, or on the role of the company or the individual in society. The statements of a company under investigation must be short and not lead to speculation.

In Peru, confidential information about an investigation is usually leaked to the media when there is a case of public interest.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

It could be mandatory if the company in which the settlement has been agreed is a listed company and if the settlement, or the settled issue, is capable of having significant influence on the security of the company, its business, its financial situation or any other aspect that could be considered relevant by a reasonable investor, or that could alter the decision to sell, purchase or keep securities for a reasonable investor. If deemed mandatory, a reserved report could be made, thus the company will report the settlement to the regulator only. However, authorisation for such a report is at the regulator's discretion. Hence, if granted, full disclosure will not be required until approval of the settlement by the judge.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

The Stock Market Superintendence has scheduled the publication of guidelines to clarify what they expect from effective compliance models.

24

Romania

Gabriel Sidere[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The most recent high-profile corporate investigation relates to corruption in the information technology (IT) sector. The National Anticorruption Directorate (DNA) alleges that the general manager of the local branch of a leading global IT company received a €870,000 bribe from the representatives of partner IT companies in exchange for better offers for company products (mainly IT licences). According to the DNA, the partner companies used these special offers to win in public tenders.

In another high-profile matter, four directors of a leading Austrian company operating in the wood processing industry are currently being investigated by the Directorate for Investigating Organised Crime and Terrorism (DIICOT) in connection with alleged organised crime, bid rigging, tax evasion and illegal logging that caused €25 million in damage.

The healthcare sector is still making headlines, as one of the largest network of private clinics in Romania is being investigated for allegedly claiming amounts from the National House of Health Insurance for medical services already paid for by the patients.

Prosecutors have also targeted the insurance sector. One of the largest current investigations involves a leading Austrian insurance group, its executive board and 87 individuals in connection with alleged tax evasion (amounting to €6 million) relating to surrendering life insurance policies open on employees' names and paying the insurance premiums directly into the employees' accounts each month.

1 Gabriel Sidere is the managing partner at CMS Cameron McKenna Nabarro Olswang LLP SCP in Bucharest.

2 Outline the legal framework for corporate liability in your country.

Article 135 of the Romanian Criminal Code provides the conditions for criminal liability of legal entities. It very broadly states that corporations (other than state and public authorities) can be held criminally liable for crimes committed in furtherance of the company's scope of business, for its benefit or in its name – irrespective of the acting capacity of the individuals committing the offence. The scope of individuals who may trigger criminal liability of a company is therefore very broad – it includes: legal representatives (e.g., a director or manager), employees, agents and even third parties who commit a criminal offence for the benefit or in the name of the company.

In practice, to trigger a company's criminal liability, prosecutors focus on proving that the company either benefited from the criminal activity of the individual perpetrating the offence or that the conduct was performed by the individual within the scope of his or her services for the company (by way of an employment contract, services contract or otherwise).

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Public prosecution offices are responsible for investigating and prosecuting crimes in Romania – there is not a specialised team focused on corporate crimes. A prosecutor is competent to investigate and prosecute a criminal offence within the jurisdiction of the court to which it is attached.

Romania also has specialist enforcement institutions, such as DIICOT and the DNA, which have exclusive jurisdiction over certain types of crimes.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Law enforcement authorities can initiate investigations based on any of the following: a complaint by a prejudiced party; self-reporting by a person with knowledge about an offence; a report by a person with a management or other control function of a public institution; the prosecution office's initiative, on the basis of data available to it; or the commission of an offence being observed.

Although there is no specific threshold of suspicion required to trigger an investigation into the facts of a matter, in practice, prosecutors will launch an investigation if they can identify direct or indirect evidence that gives rise to a suspicion that a crime has been committed.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A company can challenge a subpoena or orders for production of documents before the relevant chief prosecutor or court. Prosecutors are generally given wide discretion to conduct investigations and, in practice, subpoenas are upheld. However, a warrant to search premises and seize assets cannot be challenged effectively before it is implemented.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

No. Individuals who report on others and help the authorities to trigger their criminal liability receive a statutorily provided reduction (by half) of the punishment limits for the charged crime.

In addition, there is a limited number of crimes for which the perpetrator (1) is granted immunity if he or she reports the crime before the law enforcement authorities are notified (e.g., giving a bribe or buying influence) or (2) benefits from leniency (e.g., setting up a criminal organised group, if the perpetrator helps to identify other members of the group).

7 What are the top priorities for your country's law enforcement authorities?

In recent years, Romanian law enforcement authorities have prioritised the targeting of high-level corruption cases, EU funds fraud, tax fraud and money laundering. A notable record of success was achieved in conducting investigations into allegations of corruption at the highest levels of the government, the judiciary and across the IT, energy, infrastructure, real estate and healthcare sectors.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Romania has implemented Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems (the NIS Directive) through Law No. 362/2018.

The law requires operators of essential services and providers of digital services to have adequate security measures and to report serious incidents to the competent national authority, CERT-RO. Failure to comply may result in a fine ranging from 3,000 Romanian lei to 5 per cent of the turnover for the previous year. Given the recent enactment of the law, the approach by law enforcement authorities is not yet known.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The Romanian Criminal Code has a dedicated chapter on cybercrime, which covers crimes such as illegal access to a computer system and illegal interception of computer data transmission. Computer-related fraud and forgery are also provided in different chapters.

DIICOT handles most cybercrime allegations. In 2018, DIICOT successfully indicted several individuals for cybercrimes related to ransomware attacks and man-in-the-browser/man-in-the middle threats.

Some of these indictments relied on co-operation with similar agencies in other countries, as Romania is part of the Council of Europe's Convention on Cybercrime, the only binding international instrument on this issue.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In general, Romanian criminal law applies to offences committed on Romanian territory. However, in certain situations (e.g., when the punishment limits for the alleged crime exceed 10 years' imprisonment), the Romanian Criminal Code will apply to a Romanian citizen or Romanian legal entity that commits a crime abroad (unless an applicable international treaty states otherwise).

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The principal challenges that arise in cross-border investigations are difficulties in coordinating the investigation efforts across cultures and in communicating effectively in different languages; differences in laws regarding attorney–client privilege, employee rights and data protection laws across various countries; and differences in attitudes and approaches of law enforcement authorities.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The principle of double jeopardy applies in Romania and a corporation cannot be tried for the same or a similar crime based on the same conduct and facts, regardless of whether the initial trial occurred in Romania. However, the Romanian Criminal Procedure Code provides that cases can be revised when new evidence later comes to light that proves the previous outcome of the case was not substantiated.

Romania does not have a law similar to the US 'anti-piling on' policy, but some of the guiding principles – offsetting of fines and requiring co-operation as a prerequisite – are used in practice.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements do not occur in Romania; however, at sentencing, the national authorities may take into account any sanctions imposed on companies by their foreign counterparts.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

The influence that foreign decisions have on Romanian investigations is determined largely by applicable bilateral treaties and legislation on the provision and receiving of judicial assistance between Romania and the country in question.

Romanian authorities exercise their freedom to investigate matters within their jurisdiction and have discretion in how they view foreign decisions; they also endeavour to co-operate with foreign authorities.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

As a Member State of the European Union, Romania enforces the sanctions imposed through Common Positions adopted within the Common Foreign and Security Policy. The sanctions include asset freezing, prohibition on making funds available, prohibition on certain financial actions, restrictions on services, restrictions on goods, and prohibition on arms procurement.

Recently, the European Union extended the economic sanctions targeting specific sectors of the Russian economy until 31 January 2020. Separate sanctions banning the European Union from doing businesses in Crimea have also been renewed for another year.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Romania's tax authority, the National Agency for Fiscal Administration (ANAF), is responsible for issuing blocking orders and effectively blocking funds belonging to or under the control of persons subject to international sanctions. In recent years, the number of international sanctions enforced by ANAF has been very low.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Romania authorities co-operate with their counterparts in other countries (especially other EU Member States) by exchanging data and information relevant for the purposes of enforcement.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

The EU Blocking Regulation is directly applicable in Romania and prohibits EU operators from complying with US extraterritorial sanctions and assures them that such sanctions will not be enforced in EU courts. The regulation allows EU operators to request an authorisation to comply with the targeted US laws, if the operator can demonstrate that serious damage would be caused to it or the European Union unless the applicant is allowed to comply.

The Regulation itself does not provide any penalties for the breach of its requirements. However, Member States are obliged to determine the sanctions to be imposed in the event of a breach of any relevant provision of the regulation. According to Romanian law, failure to observe the restrictions and obligations provided by EU regulations results in a fine ranging from 10,000 to 30,000 Romanian lei and confiscation of assets.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Romanian incorporated companies face a difficult decision, considering that the US extraterritorial sanctions and the EU Blocking Regulation are now directly conflicted.

Obtaining authorisation to comply with the US extraterritorial sanctions can be difficult, and a company would need to prove that it has suffered 'serious damage', which is not defined by the EU Blocking Regulation and leads to the authorisations being granted in an arbitrary manner.

If the authorisation is not granted, the relevant authorities could be alerted about the applicant's intention to do business in breach of the EU Blocking Regulation.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Internal investigations are triggered by information from various sources, such as whistleblowers, employees, internal audits, lawsuits, business partners, media reports, as well as from the prosecutor or other government authority. Audits commenced by the Romanian tax authority could bring to light wrongdoing that could create the need to investigate. Corporations must treat any allegations of misconduct very seriously.

Romanian law obliges persons who carry out control duties within a corporation to report suspected wrongdoing to the enforcement authorities. Corporations will want to conduct investigations to make an informed decision prior to self-reporting the matter to the enforcement authorities.

Information gathering

21 Does your country have a data protection regime?

The EU General Data Protection Regulation (GDPR) entered into force in all EU Member States on 25 May 2018. The GDPR has a broader scope than the former Romanian legislation and seeks to protect the personal data of all natural persons in the European Union, regardless of the geographical location of the data controller.

The GDPR is directly enforceable in Romania, without any national legislation being required. However, a law implementing the GDPR was adopted in late July 2018. This law maintains the main provisions of the GDPR but also sets forth special rules concerning the processing of genetic data, biometric data, data concerning individuals' health, national identification numbers and data concerning work relations.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The GDPR emphasises mandatory reporting obligations that require data controllers to self-report personal data breaches that may risk the rights and freedom of natural persons. In the event of a GDPR infringement, the Romanian Data Protection Authority (RDPA) can issue a reprimand or impose a fine. Under the GDPR, fines depend on the severity of the

infringement; fines for minor infringements can be up to €10 million or 2 per cent of annual global turnover, while fines for significant infringements can be up to €20 million or 4 per cent of annual global turnover.

To date, the RDPA has imposed only four fines for infringement of GDPR provisions. The biggest of these (€130,000) was applied recently to a multinational bank for failure to apply appropriate technical and organisational measures to effectively implement data protection principles, such as minimising data and integrating processing safeguards.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

There are circumstances that arise in which a company cannot process or transfer the personal data of an individual because it requires, but does not have, the consent of an individual. In most cases, lack of consent would not prevent disclosure of information to the law enforcement authority, given that the grounds for disclosure would be the need to comply with a legal obligation.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Under Romanian law, interception of employees' communications is permitted if the following requirements are met:

- the employer's legitimate interests are justified and prevail over the targeted persons' interests or rights and liberties;
- the employees were informed accordingly;
- the employer consulted the labour union or the employees' representatives prior to introducing the interception system;
- other less intruding methods did not prove effective; and
- the storage period of the data does not exceed 30 days if there is no legal provision that allows this storage or when there are no justifying cases.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

During a criminal investigation, a search warrant may only be issued by a special judge upon the prosecutor's request; during trial, a search warrant may be issued by the court, *ex officio* or upon the prosecutor's request. Search warrants must be executed within 15 days and can only be used once.

Dawn raids can be performed between 6am and 8pm, except for acts *in flagrante delicto* or when the dawn raid is being performed in a location that is open to the public outside these hours (e.g., bars and clubs).

The company being raided must be provided with the search warrant and informed that it has the right to be assisted by a lawyer. If the presence of a lawyer is requested, the dawn

raid shall be delayed until the lawyer arrives on site, but not by more than two hours from the time the company has been informed of its right to be assisted.

Only objects, documents, correspondence and evidence relating to the offence being investigated can be seized; the correspondence between suspects or defendants and their legal counsel is subject to legal privilege and cannot be seized or searched by authorities.

If a search warrant or dawn raid violates legal requirements, any evidence seized may be deemed inadmissible in criminal proceedings and companies should seek to have it excluded. Court decisions based on unlawfully obtained evidence can be overturned. Assistance during a dawn raid by external legal counsel proves extremely useful in ensuring that the prosecutors do not seize documents or assets unrelated to the investigation or that breach privilege.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

In 2016, the Lawyers' Law clarified the rules surrounding legal privilege and specified that, as far as external counsel is concerned:

- documents that include attorney–client communications or attorney notes regarding matters relating to the defence of a client cannot be viewed, taken, seized or confiscated by prosecutors; and
- attorney–client communications can only be obtained if they have been created in furtherance of an illegal or improper purpose or relate to the promotion of an illegal act such as money laundering, terrorism, drug trafficking or various other corruption crimes.

Invoking privilege is crucial in dawn raids. It is important that companies are trained in recognising documents that are subject to legal privilege and in effectively opposing attempts by the investigating authorities to access these materials. For this reason, having external counsel on the ground during a dawn raid is recommended.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Witnesses may avoid an obligation to testify in certain situations, such as when they have a family relationship with the defendant or suspect, or when medical, legal or religious circumstances give rise to confidentiality. Otherwise, during Romanian criminal proceedings, a suspect or a witness can be compelled to testify with a bench warrant. If a witness's or a defendant's answer could give rise to self-incrimination, he or she has a right to silence. Witnesses can be criminally charged with perjury if they make false statements in their testimony.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

Although whistleblowing in the private sector is not broadly regulated, whistleblowing in the public sector is. The law protects individuals who report a breach of law committed within a

public authority or state-owned company. Reporting misconduct cannot trigger disciplinary misconduct against the employee, except when the reporting is purely vexatious or in bad faith. Financial incentive schemes for whistleblowers do not exist under Romanian law.

Under the public sector legislation, a whistleblower may report misconduct relating to a defined list of crimes, including corruption and assimilated offences, offences against the financial interests of the European Union, discriminatory treatment or practices, public procurement and non-reimbursable financing.

Whistleblowers in the public sector benefit from a presumption of good faith. Upon request from a whistleblower subject to a disciplinary investigation, the authority or entity must invite the press or broadcast media and a representative of the union to the disciplinary hearing. Any sanction imposed against a good-faith whistleblower in the public sector is likely to be overturned.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

During a disciplinary investigation, employees are entitled to:

- written notice of the allegations against them before the disciplinary hearing (the notice must provide sufficient information to enable the employees to prepare a proper defence);
- 'reasonable time' between the receipt of the notice and any hearing, to prepare a defence; and
- be informed of (and exercise) the right to defend themselves and to seek assistance, either from a lawyer, or from the trade union of which the employee is a member.

At disciplinary investigations, employees may raise all arguments and provide all evidence that they wish to bring in defence. If a disciplinary hearing is held without such prior information on the scope of the allegations being investigated, and a disciplinary sanction is applied, the sanction can be overturned in court.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

When allegations of misconduct against an employee (including officers and directors, if retained under an employment agreement) are made, employers may start an investigation into the alleged misconduct.

Employers have discretion to investigate and sanction a particular case of misconduct (including where such misconduct may constitute a criminal offence).

A company cannot take any action (except for issuing a written warning) against an employee suspected of misconduct until it has conducted an internal investigation. In certain situations, employees suspected of criminal conduct may have their employment suspended, including remuneration, until a final decision is rendered in the criminal file.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

If the investigation establishes that the employee has violated a law or internal regulation, the company may impose on the employee any sanctions permitted by law or internal regulations, including dismissal, issuing a warning or demotion.

To the extent that an employee refuses to participate in an investigation relating to another employee, if the first employee has knowledge or holds evidence that is crucial to the investigation, that employee may be subject to disciplinary measures. It is unlikely, though, that an employee's refusal to participate in the disciplinary investigation of another employee would represent sufficient grounds for dismissal.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

The best practice for commencing an internal investigation is to prepare a plan establishing the scope, approach, responsibilities and steps relating to communication and disclosure, preservation of evidence, and securing witness testimony while information is still fresh in the minds of the various participants in or witnesses to the alleged misconduct. The preparation and execution of this plan are essential for a successful investigation in a manner that allows the company to argue an efficient and consistent corporate culture of compliance within the investigation, while limiting exposure and mitigating the potential risks of a formal investigation.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

In some situations, companies and individuals must report crimes, and potential crimes, to the police. For instance, any person holding a managerial position (or an oversight authority) within a public authority or entity that, in the exercise of his or her responsibilities, has acquired knowledge of the commission of a criminal offence that warrants a criminal investigation, must immediately refer the matter to the relevant criminal investigation body.

This obligation also applies to any person mandated by public authorities to perform (or oversee) a public-interest service who has, in exercising his or her responsibilities, acquired knowledge of the commission of a crime. In general, all individuals must immediately report knowledge of any offence against human life.

Additionally, persons with control functions prescribed by law must notify enforcement authorities if they become aware of information relating to potential corruption or corruption-assimilated offences. Failure to comply with these obligations is in itself a criminal offence and could result in prosecution.

Companies are not legally required to take internal steps, other than in circumstances that give rise to mandatory reporting. It is, however, both prudent and ethical to undertake steps to ensure that the offending behaviour ceases, any evidence relating to the offending behaviour is retained and protected, and future misconduct of that kind is prevented. This helps

to build a culture of compliance, and may assist the company – in a future formal investigation – to argue that it has implemented and enforced appropriate mechanisms to curb illegal conduct within the company.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Upon receipt of a subpoena, the company should immediately alert its internal compliance and central management representatives and seek legal advice from external counsel. Measures to preserve all relevant documentation and data must be taken immediately. External counsel will assist the company to minimise risks and determine the most appropriate strategy for responding to the subpoena.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Romanian law does not oblige companies to disclose the existence of an internal investigation or any contact from law enforcement agencies. Depending on the type of investigation conducted, proactive behaviour may be recommended to prevent reputational backlash arising from a press release by the investigating authority (the DNA, for example, regularly publishes reports on investigations that have started, especially if they involve high-profile cases or persons).

36 How are internal investigations viewed by local enforcement bodies in your country?

Enforcement bodies view internal investigations positively; however, due care must be taken in performing an internal investigation to ensure that it does not interfere with a prosecution investigation. Internal investigations are also a sign of a healthy corporate culture.

Sometimes, internal investigations may validate a company's position that it was unaware of, did not condone, or did not permit the conduct in question. Further, some EU doctrine provides for the mitigation of corporate liability and sanctions if an internal investigation exposes the commission of a criminal offence and allows a corporation to improve and optimise its corporate compliance programme to prevent similar offences from occurring.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Documents, information and data of any type and format are protected by attorney–client privilege when they:

- are deemed by the client to be confidential and are provided to the lawyer for the purposes of the legal advice sought;
- were created or issued by the lawyer in relation to the legal advice sought by the client; or

- are communications or correspondence between a client and lawyer (or a lawyer and another lawyer also bound by confidentiality) relating to the legal advice sought by the client, or consist of notes or comments taken or prepared by the lawyer on the basis of information relating to a particular case.

To protect the privilege and confidentiality of an internal investigation, companies should retain an external lawyer to coordinate and execute the investigation, and ensure that retention is explicit in a written agreement and registered in the lawyer's registry of contacts.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Legal privilege protects confidential communication between a lawyer and client, if the communications relate to the seeking and receiving of legal advice. For legal entities, the definition of a 'client' is limited to persons who legally represent the entity (based on the legal entity's charter), or are empowered by the entity to seek and obtain advice on behalf of the legal entity.

If communication is shared with third parties or parties who are not considered 'clients', that communication may no longer be considered confidential and loses its privilege.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Under Romanian law, communications with in-house legal counsel who are not admitted to the bar are not protected by legal privilege. A 2010 European Court decision (CJEU Case C-550/07 P *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v. European Commission*) found that, at least in terms of competition law, communication with in-house counsel is not considered to be privileged. It was found that, although in-house counsel are enrolled in a bar or law society, and are subject to professional ethical obligations, they are not as independent from their employer as external counsel. Privilege in competition matters now only applies to communications with external counsel who have been retained by a client through a written and registered agreement.

Based on this decision, it is sensible for companies to assume that any in-house counsel communication may not be protected by legal privilege.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Attorney–client privilege applies equally to advice sought from foreign lawyers as long as: the foreign attorney is properly qualified in his or her own country; an attorney–client relationship exists; and the other requirements for privilege are satisfied.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Waiving legal privilege is not a mitigating circumstance provided by law. It may fall under the wider mitigating factors relating to circumstances that reduce the gravity of the offence or the degree of risk posed by the offender, but applying this criterion is at the discretion of the court. Nonetheless, in determining the penalty applicable in a particular case, the court will consider the gravity of the offence and the degree of risk posed by the offender. Co-operating with the investigation, and being forthcoming with information (for example, by waiving legal privilege), could count towards a more lenient sentence.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

The concept of a limited waiver of privilege is not regulated. However, that should not preclude one's ability to waive privilege only with respect to certain aspects or documents.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

Maintaining confidentiality is regarded as an absolute obligation for lawyers in Romania. Therefore, even if privilege has been waived in another country, the lawyer must maintain the privilege in Romania, except when a client waives privilege specifically in relation to the lawyer or the information becomes public.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privilege does not exist in Romania.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Legal privilege can be claimed on any documents or information created, exchanged or disclosed during the professional services rendered by a lawyer, provided the client has retained the lawyer through a written agreement registered in the lawyer's registry of contracts.

This privilege will extend to lawyers' associates, employees, subcontractors, other lawyers who co-operate with the lawyer and any individual who is helping the lawyers in carrying out their jobs. However, lawyers must inform these persons of their obligation to respect the privilege. If other parties, such as accountants or experts, have been consulted but not retained by a lawyer, privilege will not apply.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Companies may gather information by interviewing witnesses during internal investigations, but there is no legal obligation on a potential witness to testify in internal investigations.

However, in practice, employees are bound to co-operate and testify in accordance with the internal code of conduct of the company, and this may be considered a facet of the broader obligation of loyalty to the employer that employees have under the law.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

If a lawyer conducts interviews to provide legal advice on a matter, the records or a report of the interviews may be privileged. However, as discussed in questions 42 and 43, this privilege may be waived in some circumstances. Best practice would see lawyers recording interview notes as their 'impression' of an interview, rather than as a verbatim transcription.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Romanian labour law does not specify how an interview of employees or third parties should be conducted. Employers should strive for fairness and transparency when conducting interviews, treat interviewees appropriately and avoid leading questions. Further, employees generally must assist in all aspects of an internal investigation, including interviews, if this obligation is included in the company's code of conduct or under the more general obligation of loyalty to employers. Confidentiality and respect for private life should also be ensured, so that information obtained in relation to other individuals is not distributed except on a need-to-know basis and is subject to appropriate confidentiality safeguards.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

There are no prescribed methods for conducting a witness interview. Companies either retain external counsel or conduct the interviews with their internal compliance teams. If external counsel is retained to conduct an interview, it is customary for the lawyer to inform employees that he or she does not represent them. Nevertheless, an employee has a right to legal representation during the interview. Also, it is customary in a witness interview to show documents to the employee if it is necessary to refresh the employee's memory.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

A variety of circumstances trigger mandatory reporting obligations. In practice, however, law enforcement authorities are primarily concerned with investigating crimes and the enforcement of reporting breaches are usually ancillary.

One of the more problematic mandatory reporting obligations comes from corruption legislation, which requires certain categories of individuals to report indications or knowledge of potential corruption, even when these may be the sole result of a purely vexatious

or unsubstantiated claim. While the intent of the legislature was to maximise reporting of suspected corruption and ensure that the reporting obligation was triggered without the need to investigate the merits of the suspicion, the mandatory reporting obligation opens the door to potential investigations by law enforcement authorities in purely speculative or bad-faith cases.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

This issue is currently the subject of public debate in Romania. The advice given to companies varies depending on the matter and requires careful assessment of a company's duties as well as the risks and benefits of self-reporting. One considerable benefit is that the relevant authorities in Romania may agree to non-criminal penalties or other benefits for self-reporting companies.

For certain criminal offences (such as giving a bribe and acquiring influence), a person (physical or legal) who reports his or her participation in a criminal offence will receive leniency under criminal law, if the self-reporting is carried out before law enforcement authorities become aware (by any other means) of the offence.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

Companies should thoroughly investigate the issue and the surrounding circumstances to be reported to ensure that they are fully aware of all the issues that may arise during a law enforcement investigation. Next, the company should assess the benefits and potential setbacks of self-reporting, including whether the self-reporting entails impunity, or acts only as a mitigating factor or counts towards a lesser penalty; the timing and content of self-reporting and its effects on the organisation's ability to conduct its business; a potential reputational backlash; or the risk of opening up the organisation to additional scrutiny. This assessment needs to be conducted carefully, with an external legal consultant who specialises in crisis and reputation management. If the company decides that self-reporting is the most appropriate action, it should prepare a communication plan and ensure it is ready to co-operate with authorities and provide any requested support.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Companies should seek external counsel's advice regarding compliance with a document production request or a subpoena. External counsel should engage in dialogue with the law enforcement authority regarding the scope of the subpoena and communicate the intent of the company to fully co-operate. Dialogue with the authority is possible and advisable; authorities may view it as a demonstration of the willingness to co-operate and an act of

good faith. If the company fails to comply with requests within an established deadline, the prosecutor may obtain a warrant to search the premises.

54 Are ongoing authority investigations subject to challenge before the courts?

A company can file requests for quashing a prosecutor's measures and orders. Such requests are reviewed and decided by the relevant chief prosecutor. In practice, challenges are filed before the relevant chief prosecutor; however, prosecutors are reluctant to uphold such challenges, unless there is a clear indication that the company's legitimate interests are harmed.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Companies should seek legal advice on legal requirements under both countries' jurisdictions and their legal counsel should provide advice that details the appropriate strategy that the company should use to respond to the subpoenas, and advise whether it is most appropriate to respond to notices or subpoenas separately or together.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

If the material is in the company's possession, the company should comply with the request for production. Companies will also be expected to comply with requests to produce material that is legally required to be held by the company, even if the company does not possess that material. If the material requested should be in the company's possession under Romanian law but is in another country, the company should search in that country. If the material is not (and should not be) in the company's possession, the company is not bound to make additional enquiries (although, if it is feasible, making additional enquiries may be a sign of active co-operation with the investigation).

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Romanian law enforcement authorities frequently co-operate with foreign law enforcement.

The Criminal Procedure Code and Law No. 302/2004 regulate Romania's co-operation procedures on extradition, European arrest warrants, the transfer of criminal proceedings and sentenced persons, and the execution of judgments. These laws and the 2000 EU Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union regulate Romania's obligations in providing and receiving mutual legal assistance, including the search, seizure and confiscation of assets.

Additionally, Romania has signed more than 25 bilateral treaties with other countries, including France, Italy and the United States, which enable it to provide and receive assistance in criminal matters.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

The law enforcement authority is itself under a duty of confidentiality with respect to material it has accessed as a result of a request for production or a search warrant. Criminal procedure rules specifically require a strict level of confidentiality with respect to all information discovered during such procedures. Moreover, (1) the unlawful disclosure of information that is not public by a person who had access to that information as part of his or her work-related duties and (2) the use of information that is not public or granting an unauthorised person access to such information, if perpetrated with the purpose of obtaining money or other undue benefits, constitute criminal offences sanctioned by imprisonment.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

In these circumstances, companies should seek an exception and inform the relevant law enforcement authority that they cannot reasonably comply with the request without violating the laws of another country. Further, as the company receiving the request would not typically own the documents in another country, the company should direct the law enforcement authorities to the foreign entity holding the documents.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Generally, a company's data is not protected under Romanian data protection statutes and, as a result, the obligation to comply with a notice or subpoena is not blocked by data protection statutes unless it involves the personal data of employees or clients (and even in those cases, restrictions on consent to disclose would most likely be overridden by other legitimate grounds). The GDPR, implemented in May 2018, has the same effect.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

Compliance with a request for production of material is mandatory under the law – to do otherwise would be to act in breach of the law. Unless there are legitimate grounds to argue that a request violates specific rights or legitimate interests of the company (in which case the company is able to file a complaint against the order), the request should be complied with.

Furthermore, if the request is not complied with, a warrant may be issued to search the company premises to obtain the requested material.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

The main criminal penalty applicable to legal entities is a fine, ranging from 3,000 to 3 million Romanian lei. The penalty can be increased by a third (up to a maximum of 3 million lei) if the company perpetrated the crime with the purpose of obtaining financial gain.

Other penalties include:

- dissolution;
- suspension of the legal entity's activity for between three months and three years;
- prohibition of the legal entity's participation in public procurement procedures for between one and three years;
- shutting down the legal entity's offices for between three months and three years;
- placing the legal entity under judicial supervision; and
- publication of the sanctioning decision.

For individuals, the main penalties are imprisonment and fines.

Individual employees, directors and the companies they serve can be prosecuted together. Criminal liability of the company does not exclude criminal liability of the individuals perpetrating the offence.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

As a general rule, a company's decision to settle in another country should be driven by pure business reasons and should therefore not be subject to any restrictions other than those regarding the lawful termination of the local entity.

However, if a company under investigation in Romania tries to move its business to another country, the prosecutor may request a judge to take a preventive measure if there is reasonable suspicion that the company perpetrated a crime and its actions are impeding the criminal investigation. In such cases, the judge has discretion to order one or more of the following measures:

- interdiction to initiate or, as the case may be, the suspension of the company's dissolution or liquidation procedure;
- interdiction to initiate or, as the case may be, the suspension of the company's merger, division or share capital reduction, started prior or during the criminal investigation phase;
- interdiction to perform certain commercial transactions that would lead to the reduction of the company's assets or that would cause the company to become insolvent;
- interdiction to conclude certain legal documents; or
- interdiction to perform activities such as those that led to the perpetration of the crime.

64 What do the authorities in your country take into account when fixing penalties?

The gravity of the offence and the threat posed by the convicted individual or company determine the severity and type of penalty. The following criteria are used to assess the gravity and threat:

- the circumstances and manner of the commission of the offence, and the means that were used;
- the threat to the protected social interest;
- the nature and seriousness of the outcome produced by the offence or other consequences of the offence;
- the reason for committing the offence and the intended goal;
- the nature and frequency of offences in the indicted person's criminal history;
- the indicted person's conduct after committing the offence and during the trial; and
- the indicted person's level of education, age, health, family and social situation.

Where the law provides for alternative penalties, the court may also use these criteria to assess which penalties are most appropriate.

When determining the value of a corporate fine, in addition to the above criteria, courts will consider a company's financial status and any benefit derived by the company as a result of the crime. The value of corporate fines has increased and have culminated at the beginning of 2019 with the biggest fine ever applied to a company in Romania. The leading television and internet provider in Romania was convicted of money laundering and fined 1.25 million Romanian lei; in addition, €3.1 million and 655,124 lei was seized.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Romanian legislation does not provide for non-prosecution agreements or deferred prosecution agreements for corporations or individuals.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Romanian legislation does not provide for non-prosecution agreements or deferred prosecution agreements for corporations or individuals.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Companies must cautiously weigh the benefits and risks of proceeding under such a settlement. Some of the factors that should be considered are:

- the strength of the prosecution case and defence case, and the likely outcome;
- the sanction that is likely to be imposed in the event of a conviction;

- the object of the settlement and an assessment of whether the settlement is comprehensively defined;
- the effect the settlement may have on any aspect of the company's future activities and operations;
- ensuring the settlement is consistent with the company's internal regulations; and
- consideration of any benefits derived, such as the potential for a guilty plea to act as a mitigating factor in sentencing.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Romanian legislation does not provide for external corporate compliance monitors.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Parallel civil actions are allowed; however, in practice, they are often suspended until the conclusion of the criminal proceedings, because findings of fact in criminal courts may influence civil courts.

Parties to civil matters do not have access to authorities' or criminal investigation files unless they also hold a capacity in the criminal file (i.e, injured civil party); that is because investigations must maintain confidentiality and are not made public.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

The procedure and information obtained during criminal investigations is not public. Moreover, during the course of a criminal investigation, the prosecutor may restrict access to the case file if access could prevent a proper criminal investigation. Once official charges are brought against a person, access can be restricted for a maximum of 10 days.

Once a case is before a court, the criminal investigation and subsequent information becomes public (although the court may, in limited circumstances, judge the file in chambers, without public access). This does not mean that the entire file is generally accessible to the public, and requests may be made on the basis of Romanian regulations on freedom of access to information.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

The appointment of a public relations advice team is crucial to develop and follow a well-planned strategy. Relevant stakeholders, experts and legal consultants should work together to prepare public statements and to avoid damaging the company's reputation.

72 How is publicity managed when there are ongoing related proceedings?

Strategic considerations are required to successfully manage public communication in cases of ongoing proceedings. During the court proceeding phase, media access to information about the activity of the court and prosecutors' offices is determined by judicial authorities. It is useful for companies to have an organised plan for dealing with media queries and communications relating to the proceedings.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Disclosure by the company to the market is not mandatory and the decision must be made depending on the facts of the individual case, and by weighing up the factors discussed in question 33.

However, all decisions in criminal matters (including court-approved settlements) become public and are published on a court database. This publication is limited to basic information, such as names, the offence committed and the sanction imposed. As mentioned in question 62, a company may be required – once convicted of an offence – to ensure publication in national media of the full court decision, at the company's own expense.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

Some changes have been announced in relation to the Criminal Code that may affect legal entities. One of these targets the reduction of the statute of limitations for corruption crimes from eight to six years. The aim of these changes is to sanction the slow manner in which criminal investigations have been performed in Romania in recent years.

Another change that may affect legal entities relates to tax evasion crimes. The proposed change provides that, if a perpetrator repays the damage caused to the state budget (plus 20 per cent, interest and delay penalties), the criminal tax evasion charges will be dropped.

It is unclear if and when these changes may occur. The Constitutional Court of Romania decided that they are unconstitutional and Parliament now has to modify them and restart the procedure.

25

Singapore

Danny Ong and Sheila Ng[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The highest-profile corporate investigation currently under way in Singapore relates to the revelation that S$33 million belonging to the Singapore Exchange catalyst-listed precision engineering firm Allied Technologies Ltd, which was held in escrow with law firm JLC Advisors LLP, had gone missing. The Law Society of Singapore is carrying out an investigative audit on the law firm's client accounts.

In the meantime, the managing partner of JLC Advisors, Jeffrey Ong, has been charged with one count of cheating another company, CCJ Investments, out of S$6 million and eight counts of forgery for the purpose of cheating in the same case. It has also been revealed that three more clients of JLC Advisors have come forward to the police regarding missing monies totalling S$16 million that were held by the law firm.

This is the largest amount of alleged misappropriation involving a lawyer in Singapore since the case in 2006 involving an alleged misappropriation of S$11 million by another lawyer, David Rasif. Following this latest incident, the Law Society has said that it may consider introducing rules and guidelines for operating escrow accounts after it completes its probe into JLC Advisors.

2 Outline the legal framework for corporate liability in your country.

Corporate entities can be held criminally liable. The Interpretation Act (Cap. 1) expressly states that a 'person' includes 'any company or association or body of persons, corporate or unincorporate' unless the relevant legislation expressly provides otherwise or there is

1 Danny Ong and Sheila Ng are partners at Rajah & Tann Singapore LLP.

something in the subject or context inconsistent with such a construction. As such, a corporate entity can be charged with an offence, whether or not the legislation refers specifically to corporate entities.

This is also borne out in Singapore's main criminal legislation, the Penal Code (Cap. 224), which provides expressly that 'persons' liable to punishment under the Penal Code include 'any company or association or body of persons, corporate or unincorporate'.

There are also various pieces of legislation that contain offences specifically directed at corporate entities. For example, criminal liability can arise on the part of a corporate entity for market misconduct under Part X of the Securities and Futures Act (Cap. 289) (SFA) if the offence is committed by an employee or an officer of a corporate entity with the consent or connivance of the corporate entity and for the benefit of that corporate entity (section 236B), whereas a corporate entity may be liable to an order for a civil penalty if the corporate entity fails to prevent or detect a contravention, if that contravention is committed for the benefit of the corporate entity and is attributable to the negligence of the corporate entity (section 236C).

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The Accounting and Corporate Regulatory Authority (ACRA) is the national regulator of business entities, public accountants and corporate service providers. ACRA's Compliance Division, comprising the Enforcement Department and the Prosecution Department, undertakes investigations and prosecutions of breaches of various laws under ACRA's purview, including the Companies Act (Cap. 50).

The Monetary Authority of Singapore (MAS) is the central bank. It administers and enforces the SFA. Apart from the prosecution of criminal offences under the SFA, MAS is also responsible for the enforcement of civil penalties for market misconduct and for supervising financial institutions.

The Singapore Exchange Regulation Pte Ltd is an independent regulatory subsidiary of the Singapore Exchange (SGX), which oversees the regulation of companies listed on the SGX.

The Competition and Consumer Commission of Singapore (CCCS) is the national agency that administers and enforces the Competition Act (Cap. 50B). The Competition Act empowers the CCCS to investigate and adjudicate anticompetitive activities, issue directions to stop or prevent anticompetitive activities and impose financial penalties. The CCCS is also the administering agency of the Consumer Protection (Fair Trading) Act (Cap. 52A), which protects consumers against unfair trade practices in Singapore.

The Commercial Affairs Department (CAD), which is a specialist department of the Singapore Police Force (SPF), is the principal white-collar crime investigation agency. It investigates a wide range of commercial and financial crimes, including offences under the SFA. In 2015, MAS and CAD announced a collaboration to undertake joint investigations into market misconduct offences such as insider trading and market manipulation. In March 2018, this arrangement was extended to cover all offences under the SFA and the Financial Advisers Act, to allow for greater efficiency and more effective enforcement of capital markets and financial advisory offences.

The Corrupt Practices Investigation Bureau (CPIB) is the only agency authorised to investigate corruption offences under the Prevention of Corruption Act (Cap. 241) (PCA) and other related offences. The CPIB is a government agency under the Prime Minister's Office and is independent of the SPF.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

A police officer will ordinarily initiate investigations when information about an arrestable criminal offence is received. There is no specific threshold of suspicion necessary to trigger a police investigation.

Insofar as regulators such as MAS and the SGX are concerned, the relevant legislation provides them with investigative powers.

There is no specific threshold of suspicion necessary for MAS to initiate an investigation into an alleged or suspected contravention of the SFA so long as it considers an investigation 'necessary or expedient' (section 152, SFA).

Under the SGX (Mainboard) Listing Rules, the SGX may conduct an investigation if the SGX has reason to believe that there is a possibility that any of its rules have been contravened, a written complaint is received or the SGX is of the opinion that the circumstances warrant it.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

A notice or subpoena from a law enforcement authority may be challenged by asking the court to quash it or prohibit further action by the relevant law enforcement authority.

A search warrant issued by the Singapore courts under the Criminal Procedure Code (Cap. 68) (CPC) may be suspended or cancelled if there are good reasons for doing so.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Deferred prosecution agreements (DPAs) were implemented in Singapore on 31 October 2018 through amendments to the CPC. Prosecutors can enter into a DPA with corporate offenders under which there may be no prosecution in exchange for compliance with a series of conditions. Conditions to a DPA range from producing documents to assisting in investigations. They aim not only to penalise the entity but also to ensure that the entity does not repeat the offence in the future. DPAs must be approved by the High Court and published after such approval. The High Court must be satisfied that the agreement is in the interests of justice and its terms are fair, reasonable and appropriate.

Other than DPAs, co-operation with authorities can be a significant mitigating factor. For instance, a conditional warning in lieu of prosecution was issued to Keppel Offshore & Marine Ltd in view of the substantial co-operation rendered by the company during investigations.

7 What are the top priorities for your country's law enforcement authorities?

Singapore has a zero tolerance of corruption and prides itself on its clean and incorrupt system. This continues to be a top priority.

Cybercrime and money laundering are also key priorities towards ensuring that a resilient system with high integrity is maintained for Singapore's financial institutions and the financial sector, not least because cybercrime is the fastest-growing type of transnational crime in Singapore.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

The Cybersecurity Act 2018 (No. 9 of 2018) (CSA) provides a regulatory framework with a focus on protecting critical information infrastructures and to prevent, manage and respond to cybersecurity threats. The Commissioner of Cybersecurity is empowered to oversee all aspects of cybersecurity, and may require remedial action to be taken or certain activities to cease.

The CSA operates in tandem with the patchwork of existing legislation that promotes cybersecurity, such as the Personal Data Protection Act 2012 (PDPA). Non-compliance with the PDPA or CSA may result in enforcement actions and financial penalties of up to S$1 million.

Corporations are expected to comply with sector-specific codes of practice. For instance, the Notice on Technology Risk Management issued by MAS, the Telecommunication Cybersecurity Code of Practice for major internet service providers, and the Business Continuity Readiness Assessment Framework for public sector agencies. In addition, organisations are required to protect personal data in its possession or under its control by making reasonable security arrangements under the PDPA.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Cybercrime is regulated mostly under the Computer Misuse Act (CMA). However, cybercrime can also constitute offences under the Penal Code and the PDPA. The Singapore Police Force's Technology Crime Division within the Criminal Investigation Department has wide investigative powers and works closely with Interpol in combating cybercrime internationally.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Generally, Singapore's criminal law does not have extraterritorial effect. However, there are certain offences that do have extraterritorial effect, such as corruption offences under the PCA.

The provisions of the PCA set forth extraterritorial powers to deal with corrupt acts committed by a Singapore citizen outside Singapore as though the acts were committed in Singapore (section 37, PCA).

Further, section 29 of the PCA, when read with sections 108A and 108B of the Penal Code (which deals with the abetment of corruption offences), can attach criminal liability to a person who, from Singapore, abets the commission outside Singapore of any act, in relation to the affairs or business or on behalf of a principal residing in Singapore, which if committed in Singapore, would be an offence under the PCA.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

Investigations that require the assistance of foreign authorities may be hampered by the level of international co-operation. Singapore is a party to various international conventions and treaties that facilitate the provision and obtaining of international assistance in criminal matters, including the Treaty on Mutual Legal Assistance in Criminal Matters. Some of these have been incorporated into Singapore's laws, such as the Mutual Assistance in Criminal Matters Act (Cap. 190A) (MACMA), the Corruption Drug Trafficking and Other Serious Crimes Act (Confiscation of Benefits) Act (Cap. 65A) (CDSA) and the Terrorism (Suppression of Financing) Act (Cap. 325) (TSOFA).

International co-operation between MAS and other central banks is also provided for under the Monetary Authority of Singapore Act (Cap. 186) (the MAS Act).

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Singapore laws protect against double jeopardy, that is to say a person who has been convicted or acquitted of an offence cannot be tried again for the same offence. However, the issue as to whether international double jeopardy applies in Singapore remains resolved.

Insofar as offences under the PCA are concerned, section 37(2) of the PCA addresses this situation by stating that, once proceedings in respect of an act committed outside Singapore have been commenced in Singapore, this shall be a bar to further proceedings against a person for his or her extradition for the same offence outside Singapore.

Singapore does not have any specific 'anti-piling on' policy at present. However, MAS and CAD have a Joint Investigations Arrangement to cover all offences under the SFA and the Financial Advisors Act, allowing both agencies to consolidate their investigative resources and improve effectiveness of market misconduct investigations.

13 Are 'global' settlements common in your country? What are the practical considerations?

No. The first known global resolution in relation to a Singapore company was arrived at only in December 2017.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Decisions made by foreign authorities would generally be of interest to local investigators in respect of the same matter in Singapore. It may also have a bearing on the pace of investigations in Singapore.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Singapore implements United Nations Security Council sanctions through the United Nations Act (Cap. 339) for non-financial institutions and individuals and the Monetary Authority of Singapore Act (Cap. 186) for financial institutions. The International Convention for the Suppression of Financing of Terrorism is given effect in Singapore through the Terrorism (Suppression of Financing) Act (Cap. 325), which not only criminalises terrorism financing but also prohibits any person in Singapore from dealing with or providing services to a terrorist entity, including those designated in the act.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Sanctions implemented in Singapore are enforced by the Singapore Customs, MAS and the Inter-Ministerial Committee on Terrorist Designation. Recent years have seen a rise in the number of prosecutions for sanctions violations, such as Chinpo Shipping Company being fined for transferring money that could have contributed to North Korea's nuclear-related activities in 2016; and, in 2018, T Specialist International and its director, Ng Kheng Wah, being charged in Singapore for, among other things, the supply of sanctioned luxury goods to North Korea in breach of UN sanctions against North Korea.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

Under the CDSA, a mechanism is available for financial intelligence to be shared with other financial intelligence units of other jurisdictions. Assistance may also be provided pursuant to MACMA. However, Singapore does not enforce unilateral sanctions imposed by other countries.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Singapore has not enacted any blocking legislation.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Singapore has not enacted any blocking legislation.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct are often brought to light by whistleblowers making complaints directly to companies or to law enforcement authorities.

Apart from complaints of misconduct, which may be lodged with the law enforcement authorities, reports lodged pursuant to disclosure obligations under the CDSA in respect of property that are reasonably suspected of being connected to criminal activity are called 'suspicious transaction reports'. These reports are lodged with the Suspicious Transaction Reporting Office, which is Singapore's financial intelligence unit. While these suspicious transaction reports are property-based and for the purpose of combating money laundering, the SPF may also initiate investigations into misconduct associated with the property.

Internal investigations into misconduct may also be initiated pursuant to internal or external audits conducted by a company.

Information gathering

21 Does your country have a data protection regime?

Personal data in Singapore is protected under the PDPA, which took effect in phases beginning in January 2013. The Act governs the collection, use, disclosure, transfer and security of an individual's personal data.

Certain personal information is also protected under various statutes, such as the Banking Act (Cap. 19), the CDSA and the common law of confidentiality.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The PDPA ensures a baseline standard of protection for personal data, which requires organisations to comply with the PDPA as well as common law and other relevant laws that are applied to the industry they belong to, when handling personal data in their possession.

If the Personal Data Protection Commission finds that an organisation is in breach of any of the data protection provisions in the PDPA, it may give the organisation such directions as it thinks appropriate to ensure compliance.

There are also offences under the PDPA for which an organisation or a person may be liable.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

The PDPA provides that an organisation may collect personal data about an individual with the consent of the individual or from a source other than the individual in circumstances where collection is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data.

The PDPA also provides that an organisation may use or disclose personal data about an individual without the consent of the individual where the use is necessary for any investigation or proceeding.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Communications such as emails are not considered as personal data for the purposes of the PDPA. As such, the interception of employees' communications per se is permitted insofar as it does not amount to a contravention of the CMA. Insofar as they contain personal data, interception without consent is permitted so long as the collection of the data is reasonable for the purposes of managing the employment relationship, which include monitoring how employees use company network resources.

Organisations in breach may be subject to a financial penalty of up to S$1 million in addition to civil proceedings.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Search warrants and raids on companies are features of law enforcement in Singapore.

The person granted a search warrant must conduct the search in accordance with the warrant and with the CPC, including conducting the entry and search during a period of time specified in the warrant.

A court issuing a search warrant may suspend or cancel the warrant if there are good reasons to do so.

There are also instances when searches can be carried out by the SPF even without search warrants, for example if there is reasonable cause for suspicion that stolen property is concealed and a police officer of or above the rank of sergeant has good grounds for believing that by reason of delay in obtaining a search warrant, that property is likely to be removed (section 32, CPC).

If an illegal search is conducted, the aggrieved party may make a criminal complaint for trespass or criminal force, or commence a civil claim for damages in the tort of trespass.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

There is no prescribed process to protect privileged material during a dawn raid or search. As a practical measure, the company or individual should assert privilege during the dawn raid or search itself regarding the relevant material seized by the authorities and follow up thereafter with the authorities to claim privilege over the same.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Under section 283(2) of the CPC, the court may issue a summons to compel the appearance of a witness if that person's evidence is essential to making a just decision at the close of the case for the defence, or at the end of any proceeding under the CPC. In addition, there are other statutes that confer the power on authorities to require the attendance of witnesses for examination. For instance, the MAS has the power to require persons to be examined (section 154, SFA), and evidence obtained by the MAS in this regard may be used in criminal investigations and proceedings (section 168B, SFA).

The Singapore courts are permitted to draw an adverse inference against an accused under section 261(1) of the CPC from a failure to disclose to the police facts that he or she subsequently relies on in his or her defence at trial.

There is a right against self-incrimination in Singapore under section 22(2) of the CPC whereby a person need not say anything that might expose him or her to a criminal charge, penalty or forfeiture. However, the police do not have to inform the accused of the right against self-incrimination.

An advocate, solicitor or in-house counsel would be prohibited from disclosing any communications covered by legal privilege (sections 128 and 128A, Evidence Act). Further, a person would not be permitted to produce any unpublished official records relating to the affairs of the state (section 125, Evidence Act).

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

There is no general whistleblowing law in Singapore. Listed companies are required to disclose the existence of a whistleblowing policy, but beyond this, there are no hard and fast rules, including whether a whistleblower may be financially incentivised, as to the implementation of a whistleblowing policy within an organisation.

The PCA protects whistleblowers in that no complaints of an offence under the PCA can be admitted in evidence in any civil or criminal proceeding whatsoever, and no witness shall be obliged or permitted to disclose the name or address of any informer, or state any matter that might lead to the discovery of a person's identity.

A suspicious transaction report lodged pursuant to section 39(1) of the CDSA is also confidential and cannot be admitted in evidence in any civil or criminal proceeding

whatsoever, and no witness shall be obliged or permitted to disclose the name or address of any informer, or answer any question if the answer thereto would lead, or would tend to lead to the discovery of the name or address of the informer.

Auditors are also protected from defamation suits when reporting fraud in good faith under the Companies Act.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

For employees covered under the Employment Act (Cap. 91), which generally covers all employees with certain exceptions, such as managers or executives with a monthly basic salary of more than S$4,500, the employer may suspend the employee from work during an inquiry, but any suspension cannot exceed one week and the employee should be paid at least half his or her salary during the suspension.

Employees are also protected against wrongful dismissal under common law. Directors and officers of a company are treated no differently from employees in terms of protection under common law.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

For employees covered under the Employment Act (Cap. 91), which generally covers all employees with certain exceptions, such as seafarers and domestic workers, an employer can dismiss an employee, or take disciplinary action against an employee, only on the ground of conduct that is inconsistent with the fulfilment of the express or implied terms of his or her service after due inquiry. There is no fixed procedure for an inquiry but, as a general guide, the person or persons hearing the inquiry should not be in a position that may suggest bias, and the employee who is being investigated for misconduct should have the opportunity to present his or her case.

There are no particular disciplinary or other steps that a company must take, subject to the company's own internal policies and procedures, and the terms of employment.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

Subject to the applicability of the Employment Act to employees who are covered by the Act, generally a company may terminate the employment of an employee in accordance with the terms of the employment contract. As such, subject to the terms of the employment contract, an employee may be dismissed for refusing to participate in an internal investigation.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

Yes, it is – particularly for larger-scale internal investigations. It would typically cover the objectives of the internal investigation, the scope of investigation, the identity and roles of the investigation team and any restriction or protocol on communications or information flow regarding the investigation.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

If an issue comes to light, the company should first activate its in-house legal counsel or engage external counsel (or both) to obtain advice (including in respect of any interim measures that should be taken, and its disclosure obligations, if any) and commence an internal investigation.

The company may have an obligation to report to the authorities (for example, in respect of certain specified offences under the Penal Code pursuant to section 424 of the CPC, or its obligation to file a suspicious transaction report under the CDSA) or to make any public disclosures (if it is a listed company).

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

The company would be required to comply with the notice or subpoena and should take immediate steps to obtain legal advice, and implement the identification, extraction and preservation of the relevant documents and data. The company should ideally also take steps to ensure that copies of the documents and data are made and retained.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

A listed company must make timely disclosure of any information it has concerning itself or any of its subsidiaries or associated companies that is either 'necessary to avoid the establishment of a false market in [its] securities' or 'that would be likely to materially affect the price or value of its securities' under Rule 703 of the SGX (Mainboard) Listing Rules.

An intentional or reckless failure to disclose under Rule 703 is a criminal offence under section 203 of the SFA, for which the directors of the listed company may also be liable.

There is no obligation on private companies to publicly disclose any information, including the existence of an internal investigation or contact from law enforcement officials.

36 How are internal investigations viewed by local enforcement bodies in your country?

Internal investigations are generally welcomed by law enforcement authorities. Additionally, financial institutions regulated by MAS are generally expected to conduct internal investigations in cases involving certain types of misconduct by their licensed representatives.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

A company may claim litigation privilege over investigation reports and documents created during an internal investigation if there is a reasonable prospect of litigation at the time the documents are created, and the dominant purpose for the creation of the documents over which privilege is claimed is pending or contemplated litigation.

Legal advice privilege can also be claimed for a document if there is legal advice embedded in it, or it was created for the dominant purpose of provision to legal counsel for the purpose of seeking legal advice.

To ensure that privilege is protected, legal counsel, whether external or in-house, should be substantially involved in the investigations, particularly when conducting interviews of witnesses. However, it should be noted that merely copying legal counsel in correspondence is not enough to attract privilege, and that the contents themselves have to satisfy the requirements for privilege. It would also be good practice not to mix legal and business advice in the same document, and marking advice as 'confidential and legally privileged' would assist in identifying privileged material (even though the labelling itself does not create privilege).

Generally, to ensure that the confidentiality of an internal investigation is maintained, the company should put in place a communications protocol and limit the communications, reports and any advice regarding the investigations to specified individuals within the company on a need-to-know basis.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Legal professional privilege is found in two principal forms – litigation privilege and legal advice privilege. When a document is protected by either form, it is exempted from disclosure in litigation.

Legal advice privilege attaches to legal advice and communications between a lawyer (whether in-house or external legal counsel) and a client (or the company, as the case may be in the context of an in-house legal counsel) for the purpose of seeking legal advice, whether or not litigation is contemplated.

Litigation privilege will apply to documents and communications created for the dominant purpose of pending or contemplated litigation, and if there is a reasonable prospect of litigation at the time the documents are created.

Legal professional privilege belongs to the client, regardless of whether the client is an individual or a corporate entity.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes, pursuant to section 131 of the Evidence Act (Cap. 97).

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Common law rules of legal professional privilege pertaining to foreign lawyers apply in Singapore and are effectively as extensive as legal professional privilege under section 131 of the Evidence Act.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Waiver of legal professional privilege is often viewed as a co-operative step by the authorities. There is no prescribed context in which waiver of legal professional privilege is mandatory or required. However, it is not unheard of for regulatory authorities, in certain circumstances, to request that a company waives privilege over an internal investigation report that is required to be submitted to the authorities.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Yes. For example, in a recent decision, the High Court found that in a multiparty litigation, selective disclosure to an adverse party of any documents to which litigation privilege applies does not waive the litigation privilege generally.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

This question has not been determined specifically in Singapore. However, it is noted that the concept of limited waiver of privilege exists in Singapore.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege can be used to enable party B to shield behind the privilege of party A and prevent party C from obtaining or using documents from B that were provided to B pursuant to the common interest between A and B in the subject matter of the documents.

Common interest privilege can also be used to enable A to obtain documents from B, which B can withhold on the ground of privilege against the rest of the world, on the basis that it is inconsistent with the common interest for B to claim privilege against A in relation to these documents.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Yes, if the documents created with the assistance of third parties fall within the scope of litigation privilege or legal advice privilege, for example if a document was created by a third party who was acting as the client's agent at the time, for the dominant purpose of obtaining legal advice.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

There is no prohibition against witness interviews as part of an internal investigation.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Yes, if the interview records fall within the scope of litigation privilege.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There are no specific requirements that must be adhered to for a witness interview of employees or third parties. However, it is good practice to state up-front during the interview whom the interviewers represent and, where appropriate, make it clear that they are not acting for the employee. This is to avoid any potential claims of conflict of interest.

It would also be advisable to involve legal counsel to ensure that the witness interviews are conducted with the benefit of legal advice, and to ensure that any statements taken during internal investigations may properly be protected by privilege.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Generally, an interview starts with the interviewer explaining the purpose of the interview and highlighting that the interview should be kept confidential. Questions would be asked and if these questions relate to certain documents, these documents are usually put to the witness during the interview.

When allegations are being made against an employee, it is advisable to give the employee an opportunity to seek legal advice.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Yes. Section 39 of the CDSA imposes an obligation to lodge 'suspicious transaction reports' in respect of property that is reasonably suspected to be connected to criminal activity.

Section 424 of the CPC also imposes an obligation to file a police report in respect of specified offences under the Penal Code.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting and co-operation would generally be seen as mitigating factors and would also provide an avenue for dialogue with the law enforcement authorities.

Companies should bear in mind that any self-reporting in a particular jurisdiction may trigger reporting or disclosure obligations in other jurisdictions.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

Before making any self-report, a company should first undertake an internal investigation and obtain legal advice on the scope of the company's disclosure obligations and potential liability.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

It is common, and indeed advisable, for a company to engage legal counsel upon receipt of any notice or subpoena from a law enforcement authority to seek advice on compliance therewith.

It may be possible to enter into dialogue with the authorities, depending on the nature of the investigations. It is also possible to engage in plea bargaining with the prosecutor even after charges are brought.

54 Are ongoing authority investigations subject to challenge before the courts?

It depends on whether the aggrieved persons satisfy the requirements for judicial review, and whether the relevant acts are justiciable in the first place.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

It is important to ensure that a consistent position is taken across the various investigations in the different countries. To this end, the company may wish to engage legal counsel to coordinate the investigations.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

If the material is in the possession or power of a company, the company must search for and produce the material, wherever that material may be located but provided that the material actually belongs to the company.

Issues might arise in circumstances where the data servers or material are maintained by third parties or related companies not in Singapore. In these circumstances, the Singapore company may nonetheless choose to co-operate and offer assistance to provide access to these data servers or materials.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Yes, this is provided for under MACMA, the CDSA, the TSOFA and the MAS Act (see question 11).

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Generally, yes, depending on the relevant legislation empowering the investigations. See, for example, part VC of the MAS Act relating to assistance to foreign authorities and domestic authorities for their supervisory and other actions in respect of money.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

The company should obtain legal advice from counsel in the foreign country to ascertain the potential liability if the documents were produced, and have its foreign and local legal counsel work together to explore a solution or establish whether it would be possible to resist the production or mitigate its exposure overseas.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

No, but Singapore has general statutory provisions that prevent disclosure of matters relating to state interests.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

In practice, the law enforcement authorities generally maintain the confidentiality of material provided to them, whether voluntarily or because they are compelled to do so.

However, foreign law enforcement authorities may request assistance and the sharing of information or documents, whether informally or formally, pursuant to the relevant legislation or treaties. Confidentiality measures may be put in place for the sharing of such information or documents. For example, assistance provided by MAS under the MAS Act in some circumstances requires the receiving authority to provide an undertaking to protect the confidentiality of information or documents.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

If a company is found guilty of a criminal offence, the typical penalty is a fine.

A company's directors, officers or employees found guilty of a criminal offence may generally be subject to imprisonment or fines.

Further, a company or individual found guilty of a criminal offence may be required by a court to pay compensation.

Other than criminal and civil liability, companies or their directors, officers or employees may also be subject to sanctions or civil penalties imposed by regulatory bodies such as the SGX and MAS.

A court may also order a third party who has benefited from misconduct to disgorge benefit arising from that misconduct, on the application of MAS or any other claimant pursuant to section 236L of the SFA.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

The Standing Committee on Debarment (SCOD) decides all cases of debarment. The relevant grounds for debarment from government contracts include:

- cheating or attempted cheating;
- giving false information that has a material bearing on the award or performance of the contract;
- corruption in connection with a government agency or contract;
- compromise of national security or public interest;
- repeated defaults; and
- bid rigging.

Except for cases involving CPIB or CCCS investigations, government agencies generally would warn the defaulting companies in writing of the intention to debar them and

the grounds for such an action before a case is submitted to SCOD. This would give the defaulting contractor the opportunity to make a business trade-off between proceeding with the contract or facing the possibility of debarment. The defaulting contractor will also be given an opportunity to explain why it has defaulted.

64 What do the authorities in your country take into account when fixing penalties?

There are various mitigating factors that may be taken into account by a court when considering an appropriate sentence, including:

- co-operation with the authorities;
- self-reporting;
- remediation;
- lack of record; and
- voluntary restitution or compensation.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Singapore has recently enacted a framework for DPAs, which came into force on 31 October 2018. Under this framework, the public prosecutor can agree to dismiss the charges a company faces provided it agrees to undertake certain obligations. A DPA would be subject to approval by the High Court, which must be satisfied that the agreement is in the interests of justice and that the terms are fair, reasonable and proportionate.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Section 149J of the CPC confers powers on the High Court to order that public notice of the DPA be postponed until the conclusion of criminal proceedings, that any information contained in the court documents be removed or redacted, or that such information shall not be published.

Material obtained by the public prosecutor in the course of negotiations for a DPA may be used against the subject of the DPA or any other person in criminal proceedings.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

If the company has a presence overseas, it should consider the implications of the settlement on any ongoing or pending investigation in respect of the same or similar subject matter overseas.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

A possible condition under a DPA could be for the appointment of a person to advise and report on the subject's compliance programmes.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Civil proceedings can continue in parallel with criminal investigations or proceedings. However, it is common to put civil proceedings on hold until the conclusion of any criminal investigation.

There is no obligation on the authorities to provide civil litigants with access to their files.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Anyone who intentionally publishes any matter or carries out any other act that prejudices, interferes with or poses a 'real risk of prejudice' to current court proceedings is liable to be found guilty of contempt of court pursuant to the Administration of Justice (Protection) Act 2016.

Further, obstruction of justice is an offence under section 204A of the Penal Code.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Depending on the scale of the matter, a company may choose to engage an external public relations firm if it does not have an in-house public relations or communications team. It is also common for external counsel to assist and advise a company on a holistic crisis management plan.

72 How is publicity managed when there are ongoing related proceedings?

Generally, a company undergoing investigation or legal proceedings tends not to comment on it when asked by the media, save to the extent necessary to meet disclosure obligations or to refute any inaccuracy. It is important that a crisis management plan is created and abided by, particularly if there are various stakeholders in the company.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

A settlement may fall within the scope of information that a listed company is required to disclose under Rule 703 of the SGX (Mainboard) Listing Rules, subject to any disclosure obligations imposed by the relevant law enforcement authorities.

Anticipated developments

74 **Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?**

On 6 May 2019, the Criminal Law Reform Bill was passed in Parliament, introducing, among other things, a new offence of fraud, adapted from the UK Fraud Act 2006. This offence focuses on the dishonest or fraudulent intent to deceive a victim, rather than the effect of the deception of the victim. With this new fraud offence, sophisticated deceptive schemes in which wrongful gain or loss was intended without an identifiable victim being deceived would now constitute an offence under Singapore law.

The Criminal Law Reform Bill also introduces provisions to tackle crime committed in the virtual arena, such as setting out a comprehensive definition of property to cover virtual currency, as well as clarifying that a company is capable of being deceived or induced to act in a certain manner for the purposes of the offence of cheating, even if none of its individual officers, employees or agents is personally deceived or induced to act in such a manner.

The Criminal Law Reform Bill has yet to come into effect.

26

Switzerland

Flavio Romerio, Claudio Bazzani, Katrin Ivell and Reto Ferrari-Visca[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

In the past few years, Switzerland has been confronted with several multi-jurisdictional investigations relating to corruption, fraud, money laundering and tax evasion. Most of these cases attracted considerable media attention.

Beginning in 2008, the US authorities, and later the Swiss Financial Market Supervisory Authority (FINMA), initiated investigations against several Swiss banks in connection with their US cross-border business. By the end of 2018, more than 90 Swiss banks had reached an agreement with the US authorities and paid penalties totalling more than 6 billion Swiss francs.

Notable also are the investigations launched by FINMA and the Office of the Attorney General (OAG) in connection with the global money-laundering scandal around the Malaysian sovereign wealth fund 1MDB, and the investigations around the FIFA corruption scandal and the diesel emissions fraud scandal.

In connection with Brazil's biggest corruption case – *Odebrecht/Petrobras* (*Operation Car Wash*) – the Swiss prosecutors and FINMA have sent disclosure orders to more than 40 Swiss banks and seized assets of more than US$1 billion. By the end of 2018, the Swiss authorities were able to transfer more than 300 million Swiss francs to the Brazilian authorities. In 2018, the OAG initiated criminal proceedings against two Swiss banks.

At the national level, notable cases are the investigations in connection with possible irregularities regarding certain private and business dealings of the former chief executive

1 Flavio Romerio, Claudio Bazzani and Katrin Ivell are partners and Reto Ferrari-Visca is an associate at Homburger.

officer of Raiffeisen Bank and the investigation regarding incorrect accounting practices of the state-owned post bus company that had led to receipt of considerably higher subsidies than would otherwise have been due to it.

2 Outline the legal framework for corporate liability in your country.

Corporate criminal liability in Switzerland can arise in two situations. First, a corporation will be held criminally liable if it is not possible to attribute an offence to any specific individual because of the inadequate organisation of the corporation. Second, a corporation may be held criminally liable if it fails to take all necessary and reasonable organisational measures to prevent certain offences, such as bribery, corruption, financing of terrorism or money laundering. The penalty is a fine up to 5 million Swiss francs.

Corporations may also be fined in administrative criminal proceedings instead of the responsible individual if a penalty of no more than 5,000 Swiss francs will be imposed and the investigations would be disproportionate compared to the fine. If the matter concerns a violation of financial market laws, the fine may be as high as 50,000 Swiss francs.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

There are no specific law enforcement authorities regulating corporations. Accordingly, there are no specific policies or protocols relating to the prosecution of corporations.

At cantonal level, criminal laws are enforced by the regional and cantonal prosecutors with the assistance of the police. Some cantons have specialist prosecutors' offices for business crimes.

At federal level, the OAG is responsible for prosecuting offences that are subject to federal jurisdiction (e.g., espionage, certain cases of corruption, international organised crime and certain white-collar crimes). The Federal Department of Finance is generally responsible for prosecuting offences against financial market laws (e.g., violation of duty to file a suspicious activity report or violation of disclosure rules).

In addition, government agencies enforce administrative laws and regulations. Important regulatory authorities at a national level are FINMA, which is responsible for monitoring financial institutions and enforcing the financial market legislation, and the Competition Commission (COMCO), which is responsible for monitoring companies for signs of anti-competitive conduct, combating harmful cartels and enforcing merger control legislation.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The police, the prosecutors and the Federal Department of Finance are required to open an investigation once they become aware of a potential criminal offence.

FINMA will initiate an investigation if it has reason to believe that financial market laws and regulations have been violated. However, FINMA has some discretion in deciding whether to open formal enforcement proceedings. For example, it may refrain from opening formal enforcement proceedings if a supervised entity fully co-operates and instantly implements all necessary remedial measures to ensure compliance with financial market legislation.

COMCO has adopted guidelines to establish the circumstances under which it will investigate antitrust violations. It usually opens an investigation when an alleged violation is serious or has a significant effect on the market, or when the case raises a legal question that warrants judicial clarification. COMCO usually declines to investigate complaints when the issue could be better solved through private litigation. COMCO can also decline to investigate a complaint when the target business has already changed its policy, or when it agrees to adapt its market behaviour or contracts.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

In general, any orders from authorities can be challenged before the competent authorities and courts.

In criminal proceedings (including administrative criminal proceedings), records and objects must be sealed if the owner claims that they may not be searched or seized (e.g., owing to attorney–client privilege). The authorities then have the possibility to file a request for the removal of the seal before the competent courts.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Confessions and co-operation during the investigations in administrative criminal proceedings and criminal proceedings may lead to a reduction in the sentence. However, there are currently no specific immunity or leniency rules in Swiss criminal laws for co-operation. Therefore, an individual must carefully assess the potential benefits and downsides and decide on a case-by-case-basis whether he or she wants to co-operate with the authorities.

In enforcement proceedings, supervised entities and individuals are in general required to provide all information and documents that FINMA requests to fulfil its supervisory tasks. In this context, co-operation is not a mitigating factor but a statutory obligation. However, a supervised entity or individual is more likely to be able to negotiate an alternative resolution and to avoid formal enforcement proceedings by agreeing to co-operate with FINMA and take remedial measures.

COMCO has adopted a leniency policy that closely mirrors the model of the European Commission's programme. Companies may be granted complete or partial immunity from sanctions if they self-report, hand over all available evidence and fully co-operate with COMCO. However, only the company that first reports a cartel may benefit from full immunity. Companies reporting subsequently may receive a reduction of their fine if they provide significant additional evidence.

In tax law, voluntary disclosure may lead to a mitigation or waiver of punishment if certain requirements are met.

7 What are the top priorities for your country's law enforcement authorities?

In recent years, the focus of the Swiss law enforcement authorities has been on corruption, fraud and money laundering cases. In addition, there has been an increase in criminal proceedings in connection with cybercrime.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Currently, there is no specific legislation regarding cybersecurity. Instead, cybersecurity is regulated by a variety of Swiss laws and regulations.

According to the Federal Data Protection Act (FDPA), personal data must be protected against unauthorised processing through adequate technical and organisational measures. In general, any violations of this principle must be enforced by bringing an action before the civil courts. The Federal Data Protection and Information Commissioner (FDPIC) has currently no enforcement powers (see question 21).

Based on the Financial Market Infrastructure Act, financial market infrastructures are required to operate IT systems that ensure the availability, confidentiality and integrity of data relating to participants and their transactions. Violations of these requirements might lead to investigations or, in serious cases, to formal enforcement proceedings by FINMA. Data breaches concerning data covered by Swiss bank secrecy may result in imprisonment for up to three years or a monetary penalty of up to 540,000 Swiss francs.

Currently, there is no general statutory duty to report data breaches. Depending on the circumstances, however, it might be advisable to notify the data subjects affected by such breaches based on the general data processing rules. In addition, there are some sector-specific reporting obligations, including in the financial services, telecommunications, aviation, railway and nuclear sectors.

It is also possible (not an obligation) to inform the Swiss Reporting and Analysis Centre for Information Assurance (known as MELANI) about cyber incidents.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

There is no specific law in Switzerland that regulates cybercrime. However, there are several provisions in the Swiss Criminal Code (SCC) that are specific to cybercrime, including unauthorised obtaining of data or unauthorised access to a data processing system. Depending on the circumstances, other criminal provisions may be applicable also, such as document forgery, extortion, coercion and money laundering.

Switzerland is a member of the Budapest Convention on Cybercrime. The main objective of the Convention is to pursue a common criminal policy aimed at protecting society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Generally, the Swiss authorities have jurisdiction over offences committed in Switzerland. An offence is committed in Switzerland if either the accused person acted in Switzerland or the offence had effects in Switzerland.

In specific cases, Swiss courts also have jurisdiction over offences committed abroad, including:

- offences against the Swiss state or its national security;
- specific offences against minors (e.g., trafficking, sexual assault, rape);
- offences that Switzerland undertook to pursue based on an international treaty if the offence is also punishable in the place it was committed; and
- offences that are punishable both in Switzerland and the place abroad where it was committed if the offence in question is an extraditable offence and the accused person is located in Switzerland but not extradited.

If the offence was committed abroad, the main evidence often needs to be obtained through international mutual legal assistance, which might be a lengthy process depending on the foreign authorities. Swiss authorities are thus usually selective in the prosecution of such offences. Instead, they try to prosecute foreign offences indirectly by targeting the accused persons for related offences committed in Switzerland (in particular, money laundering).

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The typical issue in cross-border investigations is the transfer of personal data from Switzerland to foreign courts, regulators or enforcement authorities. Several legal provisions restrict the disclosure of personal data to foreign authorities, inter alia, the prohibition of unlawful activities on behalf of a foreign state (Article 271, SCC), Swiss banking secrecy (Article 47, Federal Banking Act), Swiss data protection and labour laws. Additionally, contractual secrecy obligations or confidentiality agreements may prevent the disclosure of data.

Article 271 of the SCC prohibits and sanctions activities on behalf of a foreign state on Swiss territory unless the competent administrative body has granted an authorisation. In general, Swiss-based corporations and individuals are thus required to obtain authorisation if they intend to disclose personal data to foreign authorities.

Pursuant to Article 47 of the Federal Banking Act, it is an offence to disclose confidential information relating to current or former clients of a Swiss bank. A breach of Swiss banking secrecy may not only trigger criminal sanctions but also administrative measures or proceedings and civil liability.

The FDPA requires, inter alia, that personal data only be processed in compliance with specific processing rules (see question 21). In addition, the FDPA provides that personal data may not be disclosed to recipients outside Switzerland if this seriously endangers the privacy of the data subject (Article 6, FDPA). Such a risk is presumed as a matter of statutory law if the country of destination is lacking adequate data protection regulation. The FDPIC maintains a list of countries that are deemed to have adequate data protection.

When foreign authorities use the available channels of mutual administrative or legal assistance to obtain documents and information, the aforementioned provisions do not apply.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Switzerland applies the *ne bis in idem* doctrine, which is essentially the equivalent of the double jeopardy concept in common law jurisdictions. Based on this doctrine, no person who has been convicted or acquitted in Switzerland in a final legally binding judgment may be prosecuted again for the same offence. This also applies to corporations. Owing to the territoriality principle, a foreign prosecution or conviction has, in general, no effect on the jurisdiction of Swiss criminal authorities regarding offences committed in Switzerland. Under certain conditions, however, the Swiss criminal authorities have to observe a foreign verdict of acquittal or reduce the sentence if it has already been partly served abroad.

Unless the investigations do not have the same subject matter, multiple government authorities may simultaneously investigate the same corporation. If appropriate, they usually coordinate their actions and may consult each other to ensure that their investigations do not interfere with each other or duplicate the same enquiries. The *ne bis in idem* doctrine prohibits multiple authorities from penalising companies for the same conduct. However, in general, the doctrine has no effect on civil or regulatory proceedings. Therefore, regulatory authorities may order additional measures against a corporation even if that corporation has already been convicted or acquitted in criminal proceedings.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not frequent in Switzerland. However, the Swiss authorities do co-operate with foreign authorities based on applicable laws, in particular in connection with multi-jurisdictional investigations.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

In general, Swiss authorities conduct their investigations independently. However, investigations or decisions of foreign authorities may cause the Swiss authorities to initiate an investigation.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Switzerland's sanctions programme authorises the Federal Council to impose non-military measures to implement sanctions that have been imposed by the United Nations, the Organisation for Economic Co-operation and Development or by Switzerland's most

significant trading partners (e.g., the European Union) for the enforcement of international law, in particular of human rights.

Possible sanctions are direct or indirect restrictions on transactions involving goods and services, payment and capital transfers, the movement of persons, scientific, technological and cultural exchange as well as prohibitions, licensing and reporting obligations and other restrictions of rights.

In general, Switzerland updates its sanctions lists in accordance with those issued by the United Nations.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

The State Secretariat for Economic Affairs is the main authority with responsibility for monitoring and implementing sanctions. A breach of sanctions may result in imprisonment for up to five years, which may be combined with a fine of up to 1 million Swiss francs.

SECO does not publish information on its sanctions enforcement activity. Based on our experience, however, there has not been a significant increase in sanctions enforcement activity in recent years.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

The Swiss authorities co-operate with their foreign counterparts provided that the co-operation is necessary for the implementation of the imposed sanctions regime, the foreign authorities are bound by official secrecy or a corresponding duty of secrecy, and they guarantee the prevention of industrial espionage within the scope of their activities.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Switzerland does not have restrictions in place that prohibit adherence to other jurisdictions' sanctions or embargoes. However, the blocking statutes, and secrecy and data protection regulations (see question 11), may restrict compliance with foreign reporting obligations relating to sanctions imposed by other countries or supranational organisations.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable (see question 18).

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

The Swiss authorities initiate their investigations in general based on their own observations, criminal or other complaints filed by victims or third parties, reports by whistleblowers,

media reports and reports from other authorities, including foreign authorities. The criminal authorities and FINMA are required to report all offences they become aware of in their official capacity. Investigations are also often triggered by suspicious activity and transaction reports filed with the Money Laundering Reporting Office of Switzerland.

Information gathering

21 Does your country have a data protection regime?

The basis of the data protection regime in Switzerland is the FDPA, which is applicable when personal data is processed in Switzerland by a federal authority or a private person (individual or entity). Personal data is defined as all information relating to an identified or identifiable person (individual or entity).

The FDPA requires, inter alia, that personal data only be processed lawfully, in good faith, in a proportionate manner and transparently. Any data processing that does not comply with these processing rules constitutes a breach of the data subject's personality rights. Such breaches are unlawful unless they are justified by the consent of the data subject, by an overriding private or public interest, or by a statutory provision of Swiss law.

The FDPA is currently under revision to bring it into alignment with the revised data protection regime of the European Union.

In addition, there are a number of additional statutory provisions that regulate or prohibit the process or disclosure of data (e.g., Swiss bank secrecy, professional secrecy, employment law).

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

The FDPIC is the relevant authority if federal authorities, individuals or entities process personal data in Switzerland. At the moment, the FDPIC only has limited powers; specifically, it has no enforcement powers and cannot impose any fines or sanctions. The FDPIC may issue recommendations that a specific method of data processing be amended or abandoned. If the party concerned does not follow the recommendation or rejects it, the FDPIC may file an action with the Federal Administrative Court. The Court's decision may be challenged before the Federal Supreme Court.

If an individual or entity wilfully fails to comply with its information, registration or co-operation obligation under the FDPA, it may receive a fine of up to 10,000 Swiss francs.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

Internal investigations must be set up in compliance with data protection laws. In practice, the most important data protection issue in connection with internal investigations is the provision that personal data may not be disclosed to recipients outside Switzerland if this seriously endangers the privacy of the data subject. Therefore, personal data may only be transferred to a country with inadequate data protection regulation if it justified by a statutory provision of Swiss law, the consent of the data subject, or an overriding public interest

(an overriding private interest does not suffice). However, Swiss courts only exceptionally acknowledge the existence of an overriding public interest.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

Based on data protection and labour laws, employees must be informed about the method, scope, period and purpose of any visual, audio or electronic monitoring. Consequently, any monitoring that is clandestine, or has not been announced in advance, is prohibited and cannot be justified by an overriding interest of the employer.

In addition, there are several criminal provisions that sanction the breach of privacy.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

In connection with investigations, dawn raids and search warrants are common tools of the authorities.

In general, houses, dwellings and other rooms not publicly accessible may only be searched with the consent of the proprietor unless a search warrant has been issued. Searches not covered by the search warrant are in general unlawful and evidence obtained in connection with such an illegal search is inadmissible unless it is essential to secure a conviction for a serious offence. Other evidence gained from that tainted evidence is in general also not admissible.

Search warrants can be challenged before the competent authorities or courts based on both the legitimacy and the scope of the search.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

A request may be made to seal privileged material, but this must be done without delay. The authorities must not search the sealed material, but they may file a request before the competent courts for the removal of the seal. The court will then review whether the claim of privilege is valid. The court's decision may be challenged before the Federal Supreme Court.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Every individual from the age of 15 and with the mental capacity to testify is compelled to testify before the criminal prosecution authorities and criminal courts unless they have the right to refuse testimony because of a personal relationship (e.g., marriage, kinship), for personal protection (self-incrimination) or to protect closely related persons (e.g., spouses,

parents, children, siblings), or owing to official secrecy or professional confidentiality (which applies to, for example, lawyers, members of the clergy, physicians).

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

There is currently no specific whistleblowing framework in existence in Switzerland; in particular, there is no specific protection for whistleblowers. A proposal of the Federal Council to improve the protection for whistleblowers was rejected by the National Council in 2019.

Based on Swiss labour law, employees are bound by a duty of loyalty towards their employers. Therefore, they risk legal consequences if they report potential misconduct publicly or to the authorities.

Swiss courts consider a dismissal in connection with whistleblowing to be abusive only if the employee first reported the offence or misconduct internally but if the management did not take appropriate remedial measures. Under Swiss labour law, even an abusive termination is valid and only entitles the dismissed employee to a financial compensation of up to six months' salary.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Under Swiss labour law, all employees have a general duty of loyalty towards their employers as well as an obligation to account for all their activities and work-product during their period of employment. Based on these provisions, it is recognised that employees have to assist with internal investigations conducted by the employer, including providing relevant documents and information, and participating in interviews. In return, employers have the obligation to safeguard the personal rights of their employees. If employees might be subject to criminal prosecution, it is in general advisable to alert them to the right not to incriminate oneself and to allow them not to respond to specific questions. However, there is no uniform opinion regarding this matter. The same applies to the question whether employees are entitled to have legal representation or a trusted adviser present during interviews.

In general, employees with high-level positions have an increased duty of loyalty towards their employees compared to other employees and thus have increased co-operation obligations in connection with internal investigations.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Under Swiss labour law, an ordinary dismissal is possible at any time without specific grounds, while an immediate dismissal requires a material ground. Based on case law, the employer is generally required to investigate the allegations of potential misconduct before dismissing

the employee. Otherwise, the dismissal might be considered as abusive and thus entitle the employee to financial compensation.

In practice, corporations tend to suspend employees from work while the investigation regarding their potential misconduct is ongoing.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

An unwarranted refusal to co-operate with an employer's internal investigation constitutes a breach of contractual duties and may entitle the employer to take disciplinary action against the non-co-operating employee, including, in serious cases, dismissal.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is common practice in Switzerland to prepare an investigation plan prior to the launch of the investigation. The plan should define in particular the subject matter (i.e., the factual and legal topics to be covered) and the scope of the investigation. Additionally, investigation plans often define investigatory steps, timeframes, resources and responsibilities as well as status and final reporting.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

There is no explicit statutory obligation to conduct an internal investigation. However, several provisions in corporate, labour, regulatory and criminal law may require a corporation to investigate potential misconduct so as to avoid liability and sanctions, or to be able to co-operate with the authorities.

Based on their duty of loyalty, employees are in general obliged to report to their superiors if they become aware of potential misconduct within the company. Management is required to inform the board of directors of any misconduct with potential material effects on the corporation.

In recent years, many corporations have introduced whistleblower frameworks that allow employees or third parties to file complaints anonymously.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Under Swiss criminal law, it is illegal to interfere with the course of justice, in particular to tamper with or destroy evidence. In addition, corporations have statutory obligations to preserve documents for certain periods (in general for 10 years). Therefore, corporations are required to have the appropriate systems and directives in place and to provide all employees

with clear instructions to prevent material from being destroyed that is subject to an order from a law enforcement authority.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Unless the company is listed on the Swiss stock exchange (see question 73), there is no obligation to inform the public about an internal investigation or an inquiry from a law enforcement authority.

36 How are internal investigations viewed by local enforcement bodies in your country?

In general, internal investigations are welcomed, or at least tolerated, by Swiss enforcement authorities as long as they do not negatively affect or impact their own investigations. Often internal investigations are a practical necessity for corporations to be in a position to respond to requests from criminal or regulatory authorities.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

In general, internal investigations conducted by Swiss attorneys are subject to attorney–client privilege. In two recent decisions, however, the Federal Supreme Court called into question the generality of that rule.

In both cases, the clients were financial institutions and the authorities claimed that the invocation of attorney–client privilege to protect the investigation report and its annexes would constitute a circumvention of statutory documentation obligations under the anti-money laundering legislation. Both decisions have been heavily criticised in the legal community.

Best practice to uphold attorney–client privilege in connection with internal investigations includes a clear definition of the scope of the investigation and a clear separation between fact finding and legal analysis and advice. If the client is subject to anti-money laundering duties, potential documentation obligations should either be part of a separate investigation stream and report, or explicitly excluded from the scope of the investigation conducted by external counsel.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

All communications between a client and an attorney (see questions 39 and 40 for certain limitations) and all work-product are subject to attorney–client privilege provided that they are related to the attorney's typical professional activities (i.e., advising and representing in legal matters). The protection applies irrespective of the location of the correspondence

and documents, that is to say the material does not need to reside with the attorney to be privileged.

In criminal proceedings, privilege cannot be invoked if the attorney is charged in the same context.

Pre-existing documents and materials created outside the scope of an attorney's engagement are not subject to attorney–client privilege.

Both the client and the attorney are deemed holders of the attorney–client privilege. This means that the client can release the attorney from the confidentiality obligation but the attorney may still refuse to disclose privileged information despite the release.

Attorney–client privilege can be invoked by both individual and corporate clients.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The attorney–client privilege only applies to external counsel. Consequently, communications between employees of a corporation and in-house counsel are not privileged in Switzerland.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

According to Swiss procedural laws, attorney–client privilege only applies to Swiss attorneys and lawyers in EU member states or the European Free Trade Association countries who are authorised to practise in Switzerland.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

Swiss authorities cannot require a client or the attorney to waive attorney–client privilege. If there is a disagreement as to whether specific material is privileged, the competent courts will decide whether the documents may be used by the authorities. If a corporation or individual under investigation seeks leniency but at the same time heavily relies on attorney–client privilege, this approach might be considered as inconsistent and thus as a lack of co-operation.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

As a general rule, attorney–client communications or work-product may be disclosed to third parties, including Swiss authorities, without waiving privilege. However, such disclosure may lead to factual loss of privilege if the proceedings are public (e.g., court hearings) or the authority is required to share the information with other Swiss or foreign authorities (e.g., mutual administrative or legal assistance). Therefore, it should be decided carefully on a case-by-case basis whether privileged information will be disclosed to Swiss authorities.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

In general, attorney–client privilege waived on a limited basis in another country can generally be maintained in Switzerland. However, the foreign-based recipient of the privileged information may share the information with the Swiss authorities without informing the privilege holder.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

The concept of common interest privileges does not exist in Switzerland. Corporations and individuals represented by separate attorneys may share information and work-product with each other without waiving attorney–client privilege under Swiss law.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Attorney–client privilege also applies to third parties assisting a Swiss attorney (or an attorney authorised to practise in Switzerland) if the third parties have been engaged by the attorney and the assistance is related to the attorney's typical professional activity (e.g., forensic analysis for advising and representing a client in administrative, civil or criminal proceedings).

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

There are no specific laws on how to conduct an internal investigation. In general, interviewing witnesses is permitted in Switzerland but interviews may only be recorded by a camera or audio device if all participants agree to the recording. Violation of this principle constitutes a criminal offence.

According to case law, Swiss lawyers may only perform interviews if there is a factual need for the interview, the interview is in the interest of the client, the lawyer avoids any influence on the interviewee and the interview does not impair investigations by the authorities. These requirements are usually met when a lawyer conducts a mere fact-finding interview in connection with an internal investigation.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Until recently, the commonly held view was that work-product created by external counsel in connection with internal investigations, including witness interviews or attorney reports, is subject to attorney–client privilege. This view has been challenged based on two recent decisions of the Federal Supreme Court (see question 37).

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

At the beginning of the interview, the interviewee should be informed about the background of the investigation, the purpose of the interview, any allegations made against the interviewee, and the intended use of the information provided during the interview (in particular whether the information may be shared with authorities). If external lawyers are present at the interview, it should be emphasised that they represent the interests of the corporation and not those of the interviewee.

The questioning should be fair, objective and based on civility and respect towards the interviewee. If it becomes apparent in the course of the interview that an interviewee may expose himself or herself to criminal prosecution, the interviewee should be informed about the right to refuse to testify and the right to seek legal representation. If the authorities are already investigating the matter, it might be advisable to liaise with them to clarify whether they have any objections to the interview.

In general, the aforementioned best practices apply to both employees and third parties. The main difference is, however, that third parties do not have an obligation to assist with an internal investigation and to participate in an interview.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

The structure of an internal interview will depend on the investigation and the person to be interviewed (for details, see questions 46 and 48). Documents will be presented to the interviewee if it is necessary or helpful for the line of questioning.

Whether or not an interviewee has a right to legal representation has not been established by the courts to date.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

There is no general statutory obligation to report potential offences or misconduct to the authorities in Switzerland.

In the financial sector, there are two main reporting obligations. First, supervised entities and individuals must inform FINMA immediately about any incident, including potential offences or misconduct within their activities, that is of material relevance for the supervision. Second, Swiss financial intermediaries are required to report cases of suspected money laundering to the Money Laundering Reporting Office of Switzerland based on applicable Swiss anti-money laundering provisions.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Among the many factors to determine whether to self-report are the likelihood that potential misconduct will become public or otherwise known to the competent authorities and the availability of a leniency regime or co-operation bonus. The decision to self-report should be made from a multinational perspective if the potential misconduct relates to more than one jurisdiction.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

Before approaching the authorities, the company should have a sufficient understanding of the relevant facts of the misconduct it plans to report. This often requires a preliminary internal investigation. In practice, it is often advisable to contact the authorities informally through external counsel.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Corporations are required to comply with notices and subpoenas unless they challenge them before the competent agencies or courts (see also question 54). There is no obligation to liaise with the law enforcement authorities before responding to notices or subpoenas. In practice, however, in many cases it is advisable to enter into a dialogue with the law enforcement authorities to get a better understanding of the background, the scope and the next steps of the investigation. A dialogue can also be helpful to clarify potential misunderstandings or ambiguities. Under certain circumstances, the authorities may be willing to amend their notices or subpoenas (e.g., when it would be practically or technically impossible or far too burdensome to provide the authorities with the information or documents requested).

54 Are ongoing authority investigations subject to challenge before the courts?

In criminal law, the initiation of investigations and preliminary proceedings is not subject to challenge before the courts unless the accused person claims that it would constitute a violation of the *ne bis in idem* doctrine (see question 12). In practice, the initiation of administrative or regulatory investigations cannot be challenged either.

Once the investigations or preliminary proceedings are ongoing, procedural orders, compulsory measures, and decisions may usually be challenged before the competent agencies or courts.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Nowadays, Swiss and foreign authorities increasingly tend to coordinate a course of action in multi-jurisdictional investigations.

Owing to several Swiss legal provisions, corporations and individuals based in Switzerland are subject to several restrictions when co-operating with foreign authorities, in particular if the requested information and documents include personal data of employees, third parties and clients (see question 11). Should a foreign authority issue a notice or subpoena, the company must carefully consider whether it may co-operate, may provide only redacted information, needs to obtain an authorisation from the Swiss authorities or should inform the foreign authority that they have to use the channels of mutual administrative or legal assistance.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In general, the Swiss authorities do not seek production of material that is only available outside Switzerland. In such cases, the Swiss authorities will rather use the available channels of mutual administrative or legal assistance to obtain the material.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Switzerland co-operates with foreign authorities based on mutual administrative or legal assistance and police co-operation through Interpol and Europol.

Whether or not assistance is granted depends on whether the applicable requirements are met. In addition, the persons concerned may challenge the decisions of the Swiss authorities to grant assistance before the competent courts.

The sharing of information with Interpol and Europol is in general not subject to challenge before the courts. However, persons may request that information related to them will be amended or deleted.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

For the confidentiality obligations of the Swiss authorities, see question 70.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

If a Swiss authority issues a notice or subpoena that would violate foreign law, the company may challenge the order before the competent authority or court. However, Swiss authorities

will usually use the available channels of mutual administrative or legal assistance (see question 56).

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Switzerland has several secrecy or blocking statutes that restrict co-operation with foreign authorities (see questions 11 and 55).

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

In general, there are no legal risks involved if the production is based on an order or subpoena issued by the Swiss authorities.

In respect of voluntary productions, however, corporations and individuals co-operating with Swiss authorities must be careful not to violate applicable data protection, labour and secrecy laws (in particular, business secrecy and bank secrecy). To reduce their exposure to risk, they can either obtain consent from the data subjects and secrecy owners, or redact the protected information.

For confidentiality regarding both voluntary and compelled productions, see question 70.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

In criminal proceedings, a corporation may face a fine of up to 5 million Swiss francs (for lesser fines in criminal administrative proceedings, see question 2). In addition, the court may order the publication of the judgment and the forfeiture or confiscation of assets.

Depending on the offence committed, directors, officers or employees may be punished with a fine (in general, up to 10,000 Swiss francs), monetary penalty (in general, up to 540,000 Swiss francs) or imprisonment (in general, up to 20 years).

In enforcement proceedings, FINMA has a wide set of enforcement tools. Inter alia, FINMA may confiscate profits generated or losses avoided through serious violations of financial market laws and regulations by supervised entities or individuals in senior functions, prohibit individuals from exercising a professional activity, withdraw licences, and order the liquidation of financial institutions in the event of serious violations. In addition, individuals and entities that do not comply with an order by FINMA may be fined up to 100,000 Swiss francs. Finally, individuals who provide FINMA with false information may face a custodial sentence of up to three years or a monetary penalty.

Some supervisory authorities (e.g., COMCO in antitrust and OFCOM in telecommunication matters) may impose fines of up to 10 percent of the average turnover of the corporation in Switzerland during the previous three years.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Debarment from government contracts is currently not a specific sanction under Swiss law. However, if a settlement with a foreign authority may have a relevant effect on the corporation's liquidity, stability, business or reputation, it is advisable to liaise with the competent supervisory authority prior to the settlement.

64 What do the authorities in your country take into account when fixing penalties?

Relevant factors for determining the fines for corporations in connection with any wrongdoing are the seriousness and number of the offences committed in their commercial activities, the damage caused by the offences, the severity of the organisational inadequacies, the economic ability of the corporation to bear the fine, remedial measures taken (e.g., restructuring measures or reparation payments), the insensitivity and quality of the corporation's co-operation with the authorities during the investigation and previous misconduct.

For individuals, the criminal authorities have to take a variety of aspects into account, inter alia, the culpability (i.e., damage caused, conduct and motives), previous conduct and the personal circumstances of the offender as well as potential mitigation factors (e.g., honourable motives, serious distress, dependency, remorse) and the effect that the sentence will have on the offender's life.

Overall, we observe a tendency by criminal authorities to impose higher fines and monetary penalties as well as longer custodial sentences for business crimes.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Neither deferred prosecution agreements nor non-prosecution agreements are available in Switzerland, either for corporations or individuals.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

No, since deferred prosecution agreements and non-prosecution agreements are currently not available in Switzerland (see question 65).

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

According to Swiss case law, journalists are entitled to access settlements with prosecutors unless the access would be contrary to overriding public or private interests. Therefore, corporations should be prepared for media enquiries and coverage once they have reached a settlement. In addition, plaintiffs may use publicly available orders against a corporation

to pursue their civil claims because most settlements include an implicit admission of guilt (e.g., payment of reparation or acceptance of the facts).

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Swiss criminal law currently does not provide external corporate compliance monitors as an enforcement tool.

However, FINMA may engage an independent and suitably qualified person as either an investigating agent or an auditing agent. Investigating agents will be engaged in connection with enforcement proceedings and are responsible for investigating the facts in connection with a potential misconduct or implementing supervisory measures ordered by FINMA. Auditing agents will conduct special audits of supervised individuals and entities.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

In connection with criminal investigations and proceedings against corporations or their (former) employees, individuals or entities claiming damages regularly request to participate as private plaintiffs. If they are admitted to participate in the criminal proceedings as private plaintiffs, they may have access to the case file, be present during hearings of parties and witnesses, ask questions of the parties and witnesses, submit requests for evidence, and file appeals against orders and the final judgment.

In administrative proceedings, however, in particular in enforcement proceedings conducted by FINMA, private plaintiffs are not parties to the proceedings and thus have no access to the case file and will not be informed about the outcome of the investigation and proceedings.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Swiss authorities and their staff are bound by official secrecy and may only disclose non-public information they become aware of during the exercise of their official duties, provided the law allows them to do so.

Investigations and pretrial proceedings conducted by the criminal authorities are not public. Therefore, the criminal authorities must treat as confidential any information gathered or received during the investigations and pretrial proceedings.

Once a case is before a court, the proceedings and the oral passing of judgments are, in general, open to the public.

FINMA does not usually inform the public about pending investigations. It only publishes information on specific proceedings when this is necessary to protect market participants, to correct wrong or misleading media reports or to maintain the reputation of the Swiss marketplace. If there is a serious violation of the law, FINMA may publish its final ruling and disclose personal data about individuals and entities.

COMCO is required to issue an official press release when opening a formal investigation stating the purpose of and parties to the investigation. COMCO may publish its decision but the publications must not reveal any business secrets. Corporations named in the decision receive the decision prior to publication and may ask COMCO to redact further information if this is necessary to protect business secrecy or personal privacy.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Communications strategies vary from company to company and will need to be assessed for each situation separately, taking into account various factors, such as the complexity and gravity of the issue or crisis. In complex or severe cases, it has become common to build a communications task force, including external counsel and communications experts, that provides guidance on the communications strategy.

72 How is publicity managed when there are ongoing related proceedings?

The communication strategy depends on the specific circumstances. In general, corporations tend not to comment on ongoing proceedings or only give very high-level comments.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

In general, there is no mandatory obligation to disclose to the market when a settlement has been reached. However, depending on the circumstances (e.g., penalty amount, effect on business), the conclusion of a settlement may lead to a disclosure obligation under the ad hoc publicity rules under which publicly listed companies have to disclose any information in their sphere of activity that could have a substantial impact on the market price.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

As mentioned in question 65, Switzerland currently has no tools that correspond to deferred prosecution agreements (DPAs) or non-prosecution agreements as known in other jurisdictions. In connection with the planned revision of the Swiss Criminal Procedure Code, the OAG proposed the introduction of a form of DPA (*aufgeschobene Anklageerhebung*). However, the Swiss Federal Council rejected the proposal in its Official Statement to the Swiss Federal Parliament dated August 2019. Therefore, it is doubtful whether DPAs will be introduced into Swiss law in the foreseeable future.

27

Turkey

Filiz Toprak Esin and Asena Aytuğ Keser[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

Since the attempted coup on 15 July 2016, criminal investigations relating to the Fethullah Gulen Terrorist Organisation (FETO) have been initiated. These investigations have also extended to corporations; those being funded by FETO or financing any associated corporation or institution, or having any kind of connection with FETO, have also been under the spotlight of the law enforcement authorities. The Financial Crimes Investigation Board (MASAK) is the organisation that has been involved to the greatest extent and has had an important role in these investigations as, in most cases, they concern financing terrorism. This involvement has resulted in new legal regulations that have extended the scope of MASAK's authority and reorganised its structure. However, it is not possible to give any detailed information about these investigations as these procedures are highly confidential and are not reported in the press.

2 Outline the legal framework for corporate liability in your country.

Under Turkish law, corporations cannot be held criminally liable. When a crime is committed for the benefit of a legal person by the participation of its representatives or authorised bodies, the Turkish Criminal Code (CC) provides for security measures to be imposed on that legal person. Those measures are listed as the cancellation of business licences granted by a public authority, and the seizure of goods that are used, allocated for or gained as a result of the commission of crime. In addition, in cases where certain crimes (e.g., fraud, collusive tendering, bribery, money laundering) are committed by representatives or authorised bodies

1 Filiz Toprak Esin is a managing associate and Asena Aytuğ Keser is a senior associate at Gün + Partners.

or by third persons who perform a task within the framework of its field of activity, administrative fines are also imposed on the legal person, as prescribed by Article 43 of the Law on Misdemeanours.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

There are no special authorities relating to the prosecution of corporations. When a crime is committed by a corporation, public prosecutors and criminal courts prosecute representatives or members of authorised bodies of the corporation. In addition, pursuant to Law No. 5549 on Prevention of Laundering Proceeds of Crime, MASAK is authorised to convey to the public prosecutor's office any case in which there is serious suspicion that a money laundering or terrorist financing offence has been committed.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Having an impression that a crime has been committed is sufficient for the public prosecutor to trigger an investigation. According to Article 160 of the Criminal Procedure Code (CPC), the public prosecutor would start an investigation as soon as he or she becomes aware of any impression of a crime being committed, by any means (e.g., the reporting of a crime).

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Whereas Law No. 2577 on Administrative Procedure provides application to a superior administrative body or the filing of a cancellation action as legal remedies to challenge the lawfulness or scope of an administrative action, the CPC provides an objection procedure before the issuing authority or its superior. The procedure to be followed when filing these applications and the time limits within which they should be made are set out clearly by these laws. Similar procedures are also set out by various special laws, such as the Law on Capital Markets and the Law on Misdemeanours.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Although it is not an agreement technically, there is an effective remorse mechanism (leniency-type mechanism) under the CC that provides for either a reduction in the punishment or full immunity. This mechanism applies for certain crimes only as prescribed by the CC; these include bribery and money laundering. In terms of bribery, if either the perpetrator, participant, intermediary or accessory to a crime reports the same to the authorities before the law enforcement bodies become aware of it, that person will not be subject to any punishment for bribery. In terms of money-laundering, there will be no punishment for a person who helps the law enforcement bodies to seize the assets that are the subject of a crime or reports their location before the commencement of criminal proceedings.

There are some reconciliation mechanisms that apply with regard to tax and customs-related administrative investigations and sanctions. These mechanisms do not provide for complete immunity, but do provide for considerable decreases in the fines and penalties imposed.

7 What are the top priorities for your country's law enforcement authorities?

In parallel with our response to question 1, the fight against terrorism has been the top priority of law enforcement authorities in Turkey. There have been amendments to several acts related to counter-terrorism and to the rules of the CPC concerning the investigation and trial procedures for such crimes.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Cybersecurity has recently become a hot topic in Turkey. According to the Electronic Communications Law, the task of determining the politics and strategies to secure national cybersecurity and to coordinate entities in the field of cybersecurity is assigned to the Ministry of Transportation and Infrastructure and the Information Technologies and Communications Institution (ITI).

In the National Cyber Security Strategy, certain sectors are listed as 'critical infrastructure sector' and cybersecurity in these (for both public and private entities) has been highlighted: electronic communication, energy, water management, critical public services, transportation, and banking and finance. The Ministry has published several sets of guidelines for the establishment of operations units for cyber incidents (OUCIs) for entities in these sectors.

ITI has been established as a regulatory and supervisory authority of the telecommunications sector and it has a significant role in providing cybersecurity within electronic communications. In this respect, the National Operations Centre for Cyber Incidents in the framework of ITI ensures co-operation between the OUCIs of other regulatory and supervisory authorities and OUCIs established within the organisation of other public and private entities in the critical infrastructure sector.

There are also some sector-specific regulations on cybersecurity; for example, the Banking Regulation and Supervision Agency has published a draft regulation for banks on standards for cybersecurity.

Regulation on cybersecurity is likely to become more detailed in the years to come. To reflect the importance of the topic for the future, the 11th Development Plan (2019–2023), published by the Turkish presidency, set targets for cybersecurity and highlights the following strategic priorities:

- improvements in technology and human resources within cybersecurity;
- establishing undergraduate and graduate programmes in the area of cybersecurity;
- raising public awareness of this matter; and
- development of a cybersecurity infrastructure.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Cybercrimes are regulated under the CC under an individual section where illegal access to a data processing system, the hindrance or destruction of a system, deletion or alteration of data and the misuse of debit or credit cards are regulated as crimes. The recording of personal data, unlawful delivery or acquisition of the same also constitutes a crime. For certain crimes, such as theft and fraud, commission of a crime through the use of a data processing system is regarded as an aggravated form of the crime. There is also a separate law regulating crimes committed via the internet (Law No. 5651).

The fight against cybercrime is undertaken by the Department of Cybercrimes, which is a unit within the General Directorate of Security. This Department was assigned as the point of contact to comply with the requirements of the EU Convention on Cybercrime, to which Turkey became a party in 2014. In addition to tasks relating to preventing and prosecuting cybercrimes, the Department has organised several workshops and educational activities to raise public awareness. In particular, the protection of children against any form of cyber-related abuse is one of the main topics about which the Department frequently publishes leaflets, brochures, etc.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In principle, the territorial scope of Turkish criminal law is limited to crimes committed within Turkey. However, trial and punishment in Turkey under Turkish laws and procedures for a crime committed in a foreign country, or by a citizen of a foreign state to the detriment of Turkey, is also possible when specific circumstances are satisfied (Articles 10 to 12, CC). Other than that, bribery can be charged as a specific crime with an extraterritorial effect in accordance with amendments to Article 252 of the CC on bribery in 2005 and 2012 in line with the process of implementation of the Organisation for Economic Co-operation and Development' Convention on Combating Bribery of Foreign Public Officials in International Business Transactions 1997 (the OECD Anti-Bribery Convention). Accordingly, Article 252 of the CC applies to:

- public officials who have been appointed or elected in a foreign country;
- officials serving in international, supranational or foreign state courts (such as judges and members of juries);
- members of international and supranational parliaments;
- persons who perform a public duty for a foreign country, including foreign public institutions;
- citizens or foreign arbitrators who are appointed to arbitrate for a dispute resolution; and
- officials or representatives of international or supranational organisations that have been established by international treaties.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

One of the main challenges that arises in cross-border investigations is the transfer of personal data pursuant to Law No. 6698 on the Protection of Personal Data (DPA) of 2016. Pursuant to Article 9 of the DPA, personal data may only be transferred abroad with the explicit consent of the data subject. However, if the general exceptions for the processing of personal data under Articles 5/2 and 6/2 exist (such as the existence of legal obligations or the legitimate interests of the data controller), personal data may be transferred abroad without explicit consent, given that the country that will obtain the data provides an adequate level of data protection or that the data controllers in both Turkey and the subject country provide a written undertaking to provide adequate protection and obtain the authorisation of the Data Protection Board. As at September 2019, the Data Protection Board has not published the countries deemed to be providing adequate protection.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Notwithstanding the fact that legal persons cannot be held criminally liable under Turkish law, the principle of *ne bis in idem* is generally recognised at national level. However, Article 9 of the CC states that a person who has been sentenced in a foreign country for a crime committed in Turkey shall be tried again in Turkey. Although Article 16 of the CC provides for the deduction of the time spent in custody or detention in a foreign country from the term of sentence to be served in Turkey, parallel investigations and even verdicts can be possible for individuals where Article 9 of the CC applies. In terms of a legal person, in spite of the exemption from criminal liability, that person may face administrative sanctions or civil liability in Turkey for the same conduct that was the subject of resolved charges in another country.

In Turkey, there is not anything analogous to the anti-piling on policy as exists in the United States.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements are not common practice in Turkey.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

There is no specific or direct rule concerning the effect of the decisions of foreign authorities on an investigation to be conducted in Turkey for the same matter. That being said, the CC allows the retrial of a person who has committed a crime in Turkey or in a foreign country if that person has undertaken an official duty on behalf of the state, even if this person has

been convicted by a foreign state court for the same matter. Naturally, the decisions of foreign authorities do not have any bearing on an investigation to be conducted for such cases. Law No. 5781 on International Private and Civil Procedural Law enables the recognition and enforcement of criminal court decisions only for verdicts concerning personal rights.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

No economic sanctions have been implemented by Turkey in recent years. That being said, for many years, Turkey has imposed sanctions on Cyprus and Armenia, such as prevention of direct transport.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Although official records show that Turkey has no direct trade with Cyprus or Armenia, it is a fact that Turkish merchants trade with these two countries indirectly. However, such relations are not strictly investigated or are not subject to any sanctions under the legislation.

So, it could be said that Turkey does not have a strict approach to sanctions enforcement.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

There is no such concept in Turkey as there is not a strict sanctions programme.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

There is no blocking legislation in force in relation to measures undertaken by third countries.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

There is no blocking legislation in force in relation to measures undertaken by third countries.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Allegations of misconduct generally come to light either through internal sources, such as employees of a company, or external sources, such as customers or distributors. Although company employees often have concerns about being identified as a whistleblower, observations show that the higher the level of misconduct, the more likely it is that employees will disclose it to their superiors. In the case of distributors, whistleblowing seems to be mostly dependent on commercial interests, as distributors are more likely to reveal misconduct

when commercial relationships have been destroyed. Internal audits are also a way of detecting misconduct.

Information gathering

21 Does your country have a data protection regime?

Yes, the DPA was enacted on 7 April 2016. Following a two-year post-adoption grace period, the Act became fully enforceable in Turkey on 7 April 2018. Moreover, Turkey is a party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108). Although Turkey has been a party to the Convention since 1981, it was not ratified until 17 March 2016.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

Pursuant to the DPA, the data protection regime is enforced by the Data Protection Board, and by criminal courts and public prosecutors for crimes regarding data protection offences.

Pursuant to Article 18 of the DPA, the Board is authorised to impose administrative fines on data controllers who breach the DPA by failing to fulfil the obligation of informing the data subject of the full scope of data processing activities, the obligations of data security, the obligation to comply with the Board's decisions and the obligation to be registered with the Data Controllers Registry. Depending on the nature of the breach of the DPA, administrative fines range from 7,352 to 1,470,580 Turkish lira and may be imposed on natural or legal persons who act as data controllers.

In April 2019, the Board imposed a fine of 1.6 million Turkish lira on Facebook because of its incapacity to block unauthorised access to the personal data of its users by some application programming interfaces, its failure to take explicit consent from the users and to duly inform the Board about the data breaches. Marriott International was fined 1.4 million Turkish lira for unauthorised access to customers' personal data within their information technology system for almost four years.

Articles 135 to 138 of the CC also regulate criminal liability regarding the data protection regime. Under the CC, the illegal recording, illegal transfer, distribution or receipt and non-destruction of personal data are regulated as criminal offences. The penalty for these offences is imprisonment for between one and four years, depending on the specific offence.

Although there is no corporate criminal liability in Turkey, security measures (see question 2) can be imposed on legal persons who commit crimes under the data protection regime.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

In a guideline announced on the DPA website with respect to data controllers and processors, attorneys are deemed to be data controllers in respect of the personal data transferred to them by their clients in relation to the legal services provided to them. Although this requirement has been highly criticised, from the perspective of the DPA, it also applies to the evidence sent to law firms by their clients. Therefore, law firms should also ensure that they comply with all the provisions of the DPA in terms of the data transferred to them by their clients.

In addition, since employees' emails fall within the scope of the DPA as personal data, seizure of such data within the framework of internal investigations is a cause for particular concern as regards data protection. Article 5 of the DPA allows the processing of personal data under certain circumstances as listed in the Article, two of which are the express consent of the data subject and the legitimate interests of the data controller. Thus, if employees did not give their express consent for the investigation of their emails, a data controller's best option would be to argue the grounds of legitimate interest for the data processing activities (i.e., internal investigations). It can be argued that processing personal data on the grounds of legitimate interest does not constitute any harm to the data subject's fundamental rights and freedom but, since this is the most abstract ground yet for data processing, data controllers should be cautious in relying on it without the explicit consent of the data subject.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

There is not a specific set of legal rules regulating this issue. However, it is approached from the perspective of data protection, right to privacy, freedom of communication and labour law, and practice is formed by the precedents of the Constitutional Court and the Court of Cassation for the time being.

To combine what is set out under these precedents, employees must be informed at an appropriate level (via employment contracts, internal regulations or any other supplement to the employment contract) that the employer can monitor their communications via company emails or phones and their consent for this must be obtained. The employer should ensure that there is a legitimate interest when taking measures that could constitute an intervention of an employee's right to privacy and that the measure is proportionate.

An intervention without these above conditions being present may result in the criminal and civil liability of the employer, and if terminations of employment contracts have been realised as a result of such an intervention, there is an increased likelihood of successful reinstatement claims.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Article 119 of the CPC stipulates that search warrants for houses, workplaces or non-public closed areas shall only be issued by a judge or a public prosecutor if a search should be carried out without delay. The warrant shall include the act constituting the grounds for the search, the subject of the search, the address where the search is to be conducted and the period for which the warrant is valid. The CPC expects the law enforcement authorities to comply with the scope and content of a search warrant in a proportionate manner. In the event of non-compliance, the subject of the warrant is entitled to compensation (both monetary and moral) from the state.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Privileged material can be lawfully protected from seizure during a dawn raid based on attorney–client privilege. The correspondence between attorneys and their clients is deemed to be a significant part of the right of defence. However, to benefit from the privilege, the correspondence must be made between an independent attorney and his or her client. Therefore, correspondence between a company and its in-house attorney cannot benefit from attorney–client privilege. To ensure the protection of privileged material during a dawn raid, it is recommended that such material be marked as confidential beforehand and that the attorney is contacted as soon as possible so that he or she can be present at the raid. This will facilitate the raising of any necessary objections while the dawn raid is being carried out. On the other hand, pursuant to the Competition Board's decision No. 15-42/690-259, dated 12 December 2015, in addition to the foregoing (i.e., the requirement for external counsel), the Board concludes that correspondence that does not fall within the scope of the right to defence and that aims to aid the violation, or that is intended to conceal a possible violation, shall not benefit from attorney–client privilege.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Pursuant to Article 48 of the CPC, an individual may refrain from providing testimony that would lead to him or her, or his or her specified relatives, being prosecuted within the scope of the right against self-incrimination. Moreover, the specified relatives of the accused also have the right to refrain from providing testimony against the accused. Besides, Article 46 of the CPC entitles individuals in certain professions (such as attorneys, healthcare professionals and financial advisers) to refrain from providing testimony regarding information relating to their profession. However, while attorneys may use their right to refrain from providing testimony under any conditions, healthcare professionals and financial advisers cannot enjoy this right if the accused waives the privilege. Pursuant to Article 44 of the CPC, if a witness who has been duly notified and summoned does not appear before the court without providing any excuse, he or she may be compelled to provide testimony before the court. Moreover, a witness who has been introduced before the court by force would also be fined for the expenses raised from his or her absence. The right against self-incrimination and the right to refrain from providing testimony are similarly regulated under Law No. 6100 on Civil Procedure.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

There is no general framework for whistleblowing in Turkey. That being said, there are financial incentives for whistleblowing relating to certain crimes. For example, whistleblowers who report tax evasion can be awarded up to 10 per cent of the tax imputed and those who

report the smuggling of goods or drugs can be awarded up to 25 per cent of the price of the smuggled goods or drugs. A recent regulation provides for whistleblowers reporting terrorist organisations also to be granted a financial incentive.

There is no legislation granting legal protection to whistleblowers. Although there is an Act on Witness Protection, it only applies to people who have provided testimonies during criminal proceedings and certain of their relatives.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

There are not any specific rules under employment law that set forth the rights of an employee (whether an officer or a director) under an investigation of any kind. Labour Act No. 4857 (LA) lists valid reasons and just causes by analogy, and being under an investigation does not constitute a reason for termination on its own. As the LA is silent on the interim period within which the investigation is conducted, most companies regulate the circumstances that apply during this period by internal policies and disciplinary regulations. As long as they are proportionate with the suspected act of the employee and his or her position regarding the misconduct, the employer may take some measures for the sake of the investigation within its right of management.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

If an employee is deemed to have engaged in misconduct following an internal investigation, the employer may proceed with terminating the employment agreement either for valid reasons or just causes, depending on the severity of the employee's conduct. However, if there are internal company policies or regulations that foresee a different sanction from termination for the specific conduct at hand, the employer is required to follow that procedure to prevent a claim for invalid termination.

If an employee is taken into custody or arrested for a period longer than notice periods within the scope of an external investigation, this constitutes a just cause for termination.

The LA only regulates termination of employment and is silent on disciplinary sanctions that could be taken during a current employment relationship. However, a company may determine disciplinary sanctions in its internal policies and regulations. From a labour law standpoint, it is especially important in drawing up internal company rules to set out the framework in a specific manner, as a sanction imposed without a clear ground may entitle an employee to several claims against the employer.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

Whether refusal by an employee to participate in an internal investigation could be a reason for termination of the employment agreement depends on the specific circumstances of the

case. If the refusal is of a nature that could be construed as a breach of the employment agreement or the employee's obligation of due care and loyalty, then it may result in dismissal.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

The methods for conducting internal investigations are still a growing area for Turkish corporations. Therefore, drawing up a document that sets out the scope of an investigation is not common. That is why it is highly recommended to have a document that can also serve as a road map of the investigation, both to have an organised and complete investigation and to keep the whole process under control. To achieve this, the document should include the purpose and scope of the investigation, the procedure to be followed and the actions to be taken (interviews with employees, examination of corporate documents or emails, etc.), the units or individuals to be involved and the means of communication with the relevant parties.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

Although its application in practice is quite rare, failure to report a crime at the very instant it has been committed, or when it is still possible to limit its consequences, constitutes a crime that is punishable by imprisonment for up to one year under the CC. Other than that, there are no mandatory reporting obligations.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

If a company receives a notice from a law enforcement authority seeking production of documents, it should comply with the notice in an appropriate way. Thus, pursuant to Article 332 of the CPC, it is obligatory to reply within 10 days to an information request raised by a public prosecutor, judge or court during the investigation and prosecution phase. If it is not possible to provide this information in due time, addressed parties must notify the appropriate person or entity why they cannot provide the information and when they will be providing it within the same period of time (i.e., 10 days). Those who do not comply with this requirement will be subject to the consequences of Article 257 of the CC, which is misconduct in office.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Only Law No. 6362 on Capital Markets sets out a disclosure obligation for information, events and developments that may affect the value and price of capital market instruments or investment decisions by investors. Article 15 of Law No. 6362 defines such cases as material events and, according to the Capital Market Board's Guidebook on Material Events,

material events include administrative and judicial proceedings that directly concern the issuer, or court actions and sanctions against those having a material duty and responsibility for the issuer.

36 How are internal investigations viewed by local enforcement bodies in your country?

In practice, the degree of importance a public prosecutor will attribute to an internal investigation very much depends on the specific circumstances of the case, and the quality and content of the findings of an internal investigation. As there is not any legal rule granting internal investigations a role in the official investigation stage, the public prosecutor and, at the next stage, the criminal court, have full discretion on how to view it.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

There are insufficient sources of specific guidance on attorney–client privilege in respect of internal investigations. Therefore, the extent to which attorney–client privilege will apply to the relationship and communications between in-house or external counsel and the perpetrators of white-collar crime remains unclear. In that respect, decisions by the Turkish Competition Board are helpful for guidance. The Board concluded that attorney–client protection covers any correspondence in relation to a client's right of defence and documents prepared within the scope of an independent attorney's legal service.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

In addition to the information in question 28, the Advocate Law of 19 March 1969 (1136) and the CPC set out the key principles of attorney–client privilege. Accordingly, the Advocate Law regulates attorney–client privilege for attorneys. According to Article 36 (Right to Keep Secrets), attorneys cannot disclose any document or information obtained while practising their profession. Similarly, Article 130/2 of the CPC sets out that any material seized as a part of a search conducted in an attorney's office must be returned immediately to the attorney if the material is understood to relate to the professional relationship between a client and that attorney. There are not any differences between an individual client and a corporation in that respect.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

There are no specific provisions that define the application of attorney–client privilege to in-house and external counsel in Turkey. However, the Turkish Competition Board stated in its *Dow* decision that correspondence with an independent attorney falls within the scope of

attorney–client privilege and shall be protected. In other words, in-house counsel employed by a corporation that is the subject of an investigation cannot enjoy attorney–client privilege.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Currently, there is no law or precedent touching on the level of privilege that a foreign lawyer will enjoy compared to a domestic one. Under the Turkish Constitution, attorney–client privilege is protected under the right to legal remedies. From the constitutional point of view, there should be no restriction to the attorney–client privilege between a client and a foreign attorney.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

There are no regulations to guide us as to whether waiver of attorney–client privilege would be regarded as a co-operative step.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

No, we do not have such a concept.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

There are no rules or regulations in this respect.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

There are no rules or regulations under Turkish law relating to common interest privileges.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

The principles of attorney–client privilege apply to the correspondence between attorney and client and not to assistance from third parties to lawyers.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

There are no rules preventing companies from interviewing witnesses as part of an internal investigation. However, obtaining consent from a witness would prevent any subsequent complaint from a criminal law or data privacy law perspective.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

There are no court cases or regulations about claiming privilege over attorney reports that are based on internal witness interviews. Therefore, good practice would be to assume privilege only when external counsel is taking notes during witness interviews or preparing attorney reports to establish a legal defence.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

There are no legal or ethical requirements or guidance under Turkish law to consider when conducting a witness interview of an employee. The general principles and provisions about data privacy law, employment law and criminal law should be adhered to during interviews (note that the latter can be an issue when, for instance, a witness claims that his or her interview took place by force and his or her freedom was restricted, or that the interview was recorded without his or her consent).

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

There is no specific format or guidance for conducting an interview. Internal interviews are usually conducted in a Q&A format. In practice, documents might be shown to the interviewees as well. Witnesses may choose to attend the interviews with their counsel.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

As stated in question 33, although its application in practice is quite rare, failure to report a crime at the very instant it is committed, or when it is still possible to limit its consequences, constitutes a crime that is punishable by imprisonment for up to one year under the CC. Other than that, there are no mandatory reporting obligations.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Self-reporting should be assessed in each case by taking into account the real risks and strategy in the matter. It would be advisable to self-report if there is an imminent threat of external investigation.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

There is no guidance on any practical steps regarding self-reporting. When a corporation or individual decides to self-report, it would be advisable also to correctly determine the relevant law enforcement body. However, note that effective remorse is available for certain crimes (e.g., bribery under the CC).

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Every communication between a law enforcement authority and a company is made in writing. However, in practice, it is advisable to have good communications with a public prosecutor to better understand the claims and status of the investigation. Other than this, there is no mechanism for plea bargaining in Turkey.

54 Are ongoing authority investigations subject to challenge before the courts?

The decision to initiate an investigation can be challenged under the procedural rules to which the authority is subject. For example, if a ministry initiates an investigation against a company, this administrative action can be challenged as per Law No. 2577 on Administrative Procedure.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

It would be advisable to have a central supervision mechanism for cross-border investigations. The consistency of negotiation packages can be affected by disclosure limitations imposed on companies through legal requirements (e.g., data protection or blocking statutes).

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

There is no specific regulation regarding production of material in a different jurisdiction. The authorities co-operate with each other, and there are some reciprocity agreements between countries that enable a request to be recognised and enforced in another jurisdiction. However, note that, in practice, it is not always quick and easy to have effective co-operation because of bureaucracy.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

Turkish authorities share information with foreign authorities through the existing bilateral and multilateral agreements on mutual legal assistance.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

As explained in question 61, any documents produced for a court file are open to third parties unless the court grants a confidentiality decision on the file.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

If compliance with a request made by an enforcement authority would violate the laws of another country, it would be advisable for that company to explain the reasons why it cannot provide the requested documentation or information to the local law enforcement authority.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Please see question 11 regarding data protection rules as blocking statutes in Turkey.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

In principle, any documents produced for a court file are open to third parties. If the relevant party submits its request for confidentiality about the material presented, it must give a legitimate reason for that request. In such a case, the court will assess whether there is legitimate and reasonable cause to ask for the material in question to be kept confidential.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

As there is no criminal corporate liability, the directors, board members or representatives of a corporation may face judicial fines or imprisonment for misconduct, but the corporation itself cannot be sanctioned. Other than this, administrative or civil liability may arise for both the corporation and any individuals concerned, in connection with misconduct.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Article 58 of Law No. 4734 on Public Procurement sets forth a suspension regime of one to two years for those who have been involved in, among other offences, collusive tendering or document forging. Moreover, Law No. 4734 sets forth that those who refrain from entering into a contract after procuring a tender will be suspended for between six months and a year. If the suspended company is an equity company, any shareholders owning more than half of its capital would also be affected by the suspension. If the suspended company owns more than half the capital of another company, that company would also be suspended accordingly.

64 What do the authorities in your country take into account when fixing penalties?

Article 61 of the CC lists the factors that a criminal judge shall consider when fixing a penalty between the lower and upper limits for the offence at hand. Those factors are the way in which the offence was committed, how the damage occurred, the severity of the perpetrator's fault, and so on. Following that, Article 62 of the CC provides the following grounds for discretionary mitigation: the background and social relations of the perpetrator; the perpetrator's conduct after the act and during the proceedings; and the possible effects of the punishment on the perpetrator's future.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Neither non-prosecution agreements nor deferred prosecution agreements are available in Turkey. Although it does not have the same scope, one may note the following.

Pursuant to Article 171 of the CPC, offences prosecuted on complaint that are subject to a penalty of imprisonment for less than one year can be deferred by the prosecutor for five years. However, certain conditions must be met before the prosecutor can make this decision. Those conditions are that the accused should not previously have been sentenced to imprisonment based on an intentional crime; the investigation should indicate that the accused will not commit any crimes after a possible deferral decision; the deferral must be more beneficial to the accused and society than prosecution; and the damage suffered by the victim and the general public must be fully compensated. If the accused does not intentionally commit a crime during the deferral period, the prosecution will be dropped.

On the other hand, Article 253 of the CPC regulates reconciliation by mediation for certain offences. In this regard, the outcomes of the offence can be compensated between the accused and the private person or entity without proceeding with a prosecution. If the offence is subject to reconciliation, the prosecutor will initiate the procedure *ex officio* and present the file to the reconciliation bureau. If all the parties agree to proceed with reconciliation, the court will defer announcement of the verdict until the conditions agreed under reconciliation are met by the accused. If the accused violates the reconciliation agreement within this period, the court will announce the verdict.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

With reference to our explanations regarding corporate liability under question 2 and non-prosecution agreements or deferred prosecution agreements under question 65, there is no such concept in Turkey.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

In Turkish law, settlement with law enforcement authorities is subject to certain requirements and limitations in terms of scope. To exemplify, penalties arising from the offence of smuggling are left out of the scope of settlement tax penalties or administrative fines. In terms of settlement for criminal liability, the possibility to settle is provided for offences, subject to a complaint by the victim, with some exceptions, such as the offence of fraud or the disclosure of business secrets, banking secrets or information relating to customers.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

There is no such concept under Turkish law. However, it is possible under the CPC for the criminal court to appoint a custodian for the management of the corporation during the investigation or criminal proceedings if the court has serious doubt that a crime has been committed and it is necessary to shed light on the material facts. That being said, the role of such a custodian is not related to monitoring and compliance with laws, but rather to financial management of the company.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Under Turkish law, the authorities' files are considered to be in the public domain and this allows access to such files by private plaintiffs. However, similar access to confidential files may be restricted.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

Article 157 of the CPC provides for the confidentiality of an investigation and Article 285 of the CC deems a breach of the confidentiality of an investigation to be an offence subject to imprisonment for between one and three years. Only the victim, the complainant and the lawyers of the parties are allowed to review the investigation file and take copies to the extent that confidentiality is maintained. After the criminal case is filed, the trials are open to the general public in principle. However, where public morality and security so requires, the

court may opt for confidential conduct of a trial. Confidentiality of a trial when the accused is less than 18 years old is mandatory.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Generally, lawyers and public relations firms work together in managing corporate communications. In sensitive cases that require communication with government bodies, in particular, lobbying firms may also take a role.

72 How is publicity managed when there are ongoing related proceedings?

When such publicity is deemed necessary by the corporation, it is mostly managed by press statements.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Mandatory disclosure in these circumstances may be required under the Law on Capital Markets, as described in question 35.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

In March 2019, the OECD issued a notice to Turkey with regard to its continued failures to implement the key aspects of the OECD Anti-Bribery Convention and to enforce its foreign bribery laws. Under this notice, Turkey is criticised about not covering state-owned or state-controlled enterprises under the current corporate liability regime. Besides, sanctions applicable to legal persons are found to be insufficient and ineffective, along with the fact that imposing a sanction on a legal person is only possible when a real person is prosecuted or convicted. The OECD clearly invited Turkey to take the necessary action to address these deficiencies under the relevant legislation and, for that purpose, set a deadline of 19 October 2019. Although several notices have been given in the past, Turkey has failed to abide by such notices and take relevant action.

The insufficiency of sanctions applicable to legal persons and the fact that they are seldom used in practice are also issues that are subject to criticism by scholars. Therefore, there might now be an increased awareness of this topic and this latest OECD notice may help to trigger legislative activity.

28

United Kingdom

Tom Stocker, Neil McInnes, Laura Gillespie, Stacy Keen, Olga Tocewicz, Alistair Wood and Rebecca Devaney[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The investigation by the UK Serious Fraud Office (SFO) into Unaoil (which involves allegations of bribery, corruption and money laundering) continues to draw interest as much for the related investigations it has spawned as for the investigation into its affairs; during summer 2019, another individual (Basil Al Jarah, Unaoil's former partner in Iraq) pleaded guilty to five offences of conspiracy to give corrupt payments.

The SFO's related investigation into the officers, employees and agents of Petrofac plc and its subsidiaries for suspected bribery, corruption and money laundering is also of interest. In February 2019, Petrofac International Limited's former global head of sales pleaded guilty to bribery. Four other senior executives were named in the charging documents but have not been charged at the time of writing. The naming of the executives without charge by the SFO has been criticised as materially prejudicial to their rights and reputation. No charges have so far been levied against a Petrofac company.

The naming of executives by the SFO also caused controversy in two deferred prosecution agreements (DPAs) concluded during 2018–2019, leading to calls for anonymity until charges are brought.

Another related investigation, into US engineering company KBR's UK subsidiary, has also raised interesting points this year, particularly on the question of the extraterritorial reach of the SFO's investigatory powers.

1 Tom Stocker, Neil McInnes and Laura Gillespie are partners, Stacy Keen and Olga Tocewicz are senior associates, and Alistair Wood and Rebecca Devaney are solicitors at Pinsent Masons LLP.

2 Outline the legal framework for corporate liability in your country.

A corporation can be held criminally liable under the laws applicable to the UK (the laws of England and Wales, Northern Ireland and Scotland, referred to collectively as UK laws) and there are several ways this can arise, depending on the factual circumstances and the types of underlying conduct.

Typically, corporate criminal offences of strict liability and offences involving a company's vicarious liability for its employees' actions arise for a range of regulatory offences under UK laws. These features of corporate criminal liability are not considered in detail in this chapter, as they tend to be less common in relation to financial crime matters, with the exception of offences involving company legislation. Generally, however, UK principles of vicarious liability of employers for the criminal conduct of employees differ markedly from the US doctrine of *respondeat superior*.

For some offences, including fraud and corruption, the law developed the 'identification doctrine' as a means of holding a corporate entity to account for its misdemeanours. In essence, this attributes the knowledge of a corporate's directing mind – the individual or individuals who control the actions of the corporate (for example, its directors, senior managers, etc.) – to the corporate itself. Whereas the idea behind the doctrine was to attribute knowledge and action to an abstract entity, in practice this has proved difficult in all but the simplest cases involving small companies with unsophisticated structures. The difficulties are particularly apparent in larger companies or multinationals with more diffuse decision-making among management teams and where complex corporate structures may mean there are numerous reporting lines that would need to be assessed. An area that frequently needs careful analysis is where management teams or business units have been given delegated authority to act on the corporate's behalf.

To meet some of the criticisms of the identification doctrine, and the consequent difficulties in holding corporates liable for misconduct, in recent years the UK has introduced two types of corporate offences, essentially holding the corporate liable for failing to prevent certain types of wrongdoing, subject in each case to the corporate being able to raise a compliance-related defence (i.e., that it had in place either adequate or reasonable procedures designed to prevent the defined type of wrongdoing occurring). One example is the Bribery Act 2010's corporate offence of failure to prevent bribery, in which a company (incorporated or carrying on part of its business in the UK) is liable for bribes paid by a third party to win business for or on behalf of the company anywhere in the world, unless it can demonstrate it had adequate procedures intended to prevent bribery. Third parties are broadly defined in the Bribery Act 2010 to include anyone who performs services for or on behalf of the company in whatever capacity (e.g., an employee, agent or intermediary). The Criminal Finances Act 2017 similarly introduced a new offence of failure to prevent the facilitation of tax evasion with an affirmative defence of reasonable prevention procedures.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

The UK has three legal systems and jurisdictions for criminal law purposes, each of which applies geographically: England and Wales, Northern Ireland and Scotland. The criminal

laws of England and Wales and of Northern Ireland are similar, whereas Scots law and procedure is markedly different.

In the UK as a whole, allegations of corporate offending involve the same criminal process, enforcement agencies and court system as investigations and prosecutions of individuals. As a corporate is a legal rather than a natural person, certain steps vary because of this status (e.g., how it may need to respond to enquiries from a regulator, how a corporate will appear in court (via counsel) and how it is sentenced if guilty of an offence). Some key law enforcement authorities involved in the regulation, investigation or prosecution of corporates in the UK include (not exhaustively) the following:

- The SFO – set up with special powers under the Criminal Justice Act 1987 for the investigation and prosecution of large and complex corporate fraud and corruption. Unusually for UK law enforcement agencies, it combines investigative and prosecution functions.
- National Crime Agency (NCA) and local police forces – tend to lead investigations involving smaller-scale or less complex fraud or corporate crime, which is then prosecuted by the Crown Prosecution Service (CPS).
- The Police Service of Northern Ireland – investigates crimes within the jurisdiction of Northern Ireland. Crimes are then prosecuted by the Public Prosecution Service of Northern Ireland (PPSNI).
- The Police Service of Scotland (Police Scotland) – investigates crimes within the jurisdiction of Scotland. Crimes are then prosecuted by the Crown Office and Procurator Fiscal Service (COPFS).
- Her Majesty's Revenue and Customs – investigates tax-related offending, which is then prosecuted by the CPS.
- Financial Conduct Authority (FCA) – the regulator of the financial services industry. As a regulator, the FCA can impose civil sanctions for misconduct, but also may prosecute regulated firms or individuals for specific market-related offences, such as insider trading and market manipulation. Frequently, cases involving financial services companies fall within the scope of both the FCA and the SFO's investigation powers. In those cases, the SFO will usually take precedence in relation to the criminal proceedings as it may prosecute a wider range of offences.
- Competition and Markets Authority (CMA) – investigates anticompetitive behaviour; it may impose civil sanctions but can also prosecute cartel offences.
- Department for Business, Innovation and Skills – this government department investigates and prosecutes activities concerning the affairs of companies, including fraudulent trading and breaches of bankruptcy or disqualification orders.
- Information Commissioner's Office (ICO) – investigates and prosecutes or imposes civil sanctions for data protection offences.
- Health and Safety Executive (HSE) and Health and Safety Executive for Northern Ireland (HSENI) – the HSE investigates and prosecutes or imposes civil sanctions for health and safety offences and works with the police on corporate manslaughter investigations. In Northern Ireland, the position is similar, except that it is the PPSNI (not the HSENI) that brings prosecutions. Prosecutions in Scotland are brought by the COPFS.
- Office of Gas and Electricity Markets – investigates and prosecutes certain criminal offences under legislation focused on the energy sector.

- Environment Agency, Northern Ireland Environment Agency and Scottish Environmental Protection Agency – investigate and prosecute environmental crime (in Scotland, the prosecution is brought by the COPFS and in Northern Ireland by the PPSNI).
- UK Office of Financial Sanctions Implementation (OFSI) – although not a prosecutor, OFSI has significant additional powers to impose financial penalties for breaches of financial sanctions measures.

In Scotland, all criminal investigations are undertaken by Police Scotland and the COPFS. Police Scotland has a dedicated economic crime unit, but investigations into serious and complex frauds are overseen by COPFS' economic crime unit. The SFO can also investigate crimes that have occurred in Scotland if they affect other parts of the UK, but it cannot prosecute cases in or from Scotland.

There can be concurrent jurisdiction between the SFO and the COPFS, particularly with respect to overseas bribery cases. In 2014, the SFO and the COPFS entered into a memorandum of understanding, which provides a framework for co-operation in cases of bribery or corruption that both organisations have (or may have) jurisdiction to prosecute under the Bribery Act 2010 and for determining 'primacy' to investigate and prosecute corporate bribery offences.

In late 2009, the SFO and the CPS published a joint guidance note for corporate prosecutions setting out general principles, and evidential and public interest factors that could be taken into account when making a prosecutorial decision in regard to a corporate. One of the public interest factors that these agencies are entitled to take into account to decide against a prosecution of a corporate is 'the existence of a genuinely proactive and effective corporate compliance programme'.

In July 2011, the COPFS published its civil settlement guidance, which encourages Scottish and other companies that have committed bribery offences within the jurisdiction of Scotland to self-report to the COPFS in return for the opportunity to resolve the case through a civil settlement mechanism. The initiative must be reviewed and approved each year by the Lord Advocate and has recently been extended until June 2020.

In February 2014, following the introduction of DPAs in England and Wales (but not Scotland or Northern Ireland) under Schedule 17 of the Crime and Courts Act 2013, the SFO and the CPS published a Deferred Prosecution Agreements Code of Practice setting out public interest factors for and against offering a corporate a non-prosecutorial resolution by way of a DPA.

In August 2019, the SFO issued its Corporate Co-operation Guidance as part of its Operational Handbook, which it will use in making charging decisions in relation to allegations of bribery and corruption.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

Law enforcement authorities must have reasonable grounds to suspect that a criminal offence has been committed to exercise their investigative powers.

The SFO may investigate any suspected offence that appears to the director of the SFO on reasonable grounds to involve serious or complex fraud. The SFO's powers to compel the production of evidence under section 2 of the Criminal Justice Act 1987 can be exercised in

any case in which it appears to the director that there is good reason to do so for the purpose of investigating the affairs, or any aspect of the affairs, of any person.

Additionally, and only in relation to possible bribery and corruption with an international dimension, the SFO may apply the even lower test under section 2A of the Criminal Justice Act 1987 of whether there is an 'appearance' that bribery and corruption may have taken place to initiate a pre-investigation (and use its powers under section 2 to determine whether a formal investigation should be undertaken). Therefore, the section 2A powers can only be exercised for the purpose of enabling the SFO to decide whether to open a formal investigation.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Depending on the authority and type of notice, it may be possible to informally agree a narrower scope of information to be produced without having to formally challenge the lawfulness or scope. Otherwise the company may challenge the lawfulness or scope of the notice or production order by way of application to court. Usually this challenge will be by way of judicial review (in Scotland, a bill of suspension), although under certain statutes it may be possible for the company to seek a hearing before the court or tribunal that had originally issued the notice or court order (where this is provided for under the applicable statute).

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

There is the possibility of immunity or leniency for individuals who assist or co-operate in the investigation or prosecution of criminal offences.

Section 71 of the Serious Organised Crime and Police Act 2005 (SOCPA) allows certain prosecutors, including the SFO, to grant any person immunity from prosecution in England and Wales or Northern Ireland by issuing a written immunity notice. The immunity notice, which will specify the criminal offences for which no proceedings can be brought, ceases to have effect if the person fails to comply with the conditions contained in the notice. The use of section 71 is relatively rare.

Section 73 of SOCPA provides a means to incentivise assistance from defendants. A defendant who, pursuant to a written agreement with a relevant prosecutor, has provided or has offered to provide assistance to an investigator or prosecutor is eligible to receive a reduction in sentence, provided a guilty plea has been tendered. Judges are required to state in open court the sentence would have been imposed but for the assistance given or offered, unless it would not be in the public interest to disclose that the sentence has been discounted.

Broadly equivalent principles relating to immunity and leniency apply in Scotland under Part 3 of the Police, Public Order and Criminal Justice (Scotland) Act 2006.

7 What are the top priorities for your country's law enforcement authorities?

International corruption and a coordinated global approach to its defeat has been a top priority for the UK government and its law enforcement authorities for the past few years, and this has been reiterated in the government's Economic Crime Plan 2019–2022, published

in July 2019, which makes significant commitments to meet the government's objective of tackling economic, white-collar and corporate crime.

A focus on tax evasion led to the introduction of a new corporate criminal offence of failing to prevent the facilitation of tax evasion, which came into force in September 2017, and there have been increasing calls to extend the 'failure to prevent' offences to other economic crime. The government is currently analysing the responses to an earlier call for evidence on this; its response is awaited. In the meantime, some high-profile committees and officers, including the UK's solicitor general, have given their support to the introduction of such an offence.

A further focus is increased transparency of the beneficial ownership of foreign companies investing in UK property or bidding for government contracts. This has prompted the introduction of a register of beneficial ownership of foreign investors, which is intended as a measure to reduce both tax evasion and the likelihood of UK properties being used to launder foreign criminal funds, to be operational by 2021.

Pursuant to the Criminal Finances Act 2017, unexplained wealth orders (UWOs) came into force on 31 January 2018. The legislation allows the High Court to make a UWO in respect of any property (valued at more than £50,000) where the Court is satisfied that there is reasonable cause to believe that the property is held by a politically exposed person who has been involved in serious crime or that a person connected with that individual is, or has been, involved in serious crime.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

Cybersecurity is regulated within the UK through a number of statutory regimes. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)), which came into force on 25 May 2018, requires that personal data is 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'. Accordingly, organisations that control personal data must have sufficient cybersecurity measures in place to protect against attack. There are mandatory reporting obligations in place where certain attacks happen.

Enforcement of the GDPR falls to the relevant supervisory authority within each European country; in the UK, this is the ICO.

Fines have been substantially increased under the GDPR, to up to 4 per cent of annual global turnover or €20 million (whichever is higher), and the ICO has indicated that it intends to use the full force of its powers for the most serious breaches.

Cybersecurity has far-reaching consequences, however, and a range of other regulators also require notification following a cybersecurity incident; these include the FCA, the Charity Commission and other professional regulatory bodies.

Cybersecurity is woven into a range of other statutory regimes. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) regulate providers of public electronic communication services. Service providers are similarly required to take appropriate technical and organisational measures to safeguard the security of their service. The PECR

also have mandatory reporting obligations but impose a shorter time frame than the GDPR; within 24 hours of becoming aware of the essential facts. Under the GDPR, mandatory personal data breach reports must be made within 72 hours of becoming aware of the breach. Powers open to the ICO in enforcing the PECR include criminal prosecution and a fine of up to £500,000.

Additionally, the Network and Information Systems Regulations 2018 (NIS), which came into force on 10 May 2018, govern the threat posed to essential network systems and seek to improve the functioning of the digital economy. NIS applies to operators of essential services and relevant digital service providers. The requirements placed on systems operators again include having appropriate and proportionate technical and organisational measures to manage risks to the security of the network. Additionally, appropriate and proportionate steps should be taken to prevent and minimise the effects of incidents.

There is a range of 'competent authorities' that regulate NIS, depending on the specific sector. A breach of NIS can result in a fine of up to £17 million and, like the GDPR, there is a time limit of 72 hours (from becoming aware) for reporting any incident which has a significant effect on the continuity of the essential service.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

The main regulations relating to cybercrime are the Computer Misuse Act 1990 (the CMA 1990), the Data Protection Act 2018 (the DPA 2018) and the Cyber Attacks (Asset Freezing) Regulations 2019 (the 2019 Regulations).

The CMA 1990 has been amended to take account of the developing nature of cybercrime. Offences can be tried summarily or on indictment with a range of maximum sentences, depending on the offence committed.

Although prosecutions have been made over many years pursuant to the CMA 1990, the ICO secured its first conviction in November 2018. The prosecution was followed by an application under the Proceeds of Crime Act and a confiscation order.

The domestic legislation that sits alongside the GDPR is the DPA 2018, section 170 of which makes it an offence to knowingly or recklessly obtain, disclose, procure or retain personal data without the consent of a data controller and, on indictment, the maximum sentence is an unlimited fine. The offence slightly augments that under the previous legislation (the Data Protection Act 1998). Prosecutions being brought by the ICO currently tend to be pursuant to the 1998 Act in view of the time it takes to investigate and prosecute an offence.

Proceeds of crime legislation can be used as part of the enforcement toolkit; in June 2019, for example, the ICO secured the conviction of a former managing director of a claims management company who had unlawfully obtained and sold personal data. He was sentenced to a fine of £1,050 but the benefit derived from the illegal activity was valued at £1,434,679.60. In view of the defendant's lack of assets, a nominal £1 order was made.

Aside from unauthorised access and use of information, cybercriminals also deploy ransomware to secure a ransom demand. The aim of the 2019 Regulations, which came into force on 11 June 2019, is to address this. Measures under the Regulations include sanctions, restrictive measures and offences connected with cyberattacks threatening the European Union or its Member States.

The 2019 Regulations apply to UK nationals or any body incorporated in the UK. They have extraterritorial effect, and their measures are also applicable to conduct wholly or partly outside the UK that is perpetrated by a UK national, or a body incorporated or constituted under UK law.

Rather like sanctions regimes, the 2019 Regulations restrict interactions with 'designated persons'. Dealing with or making funds available to such persons is a criminal offence. The maximum sentence under the 2019 Regulations is an unlimited fine, seven years' imprisonment, or both.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

The jurisdictional basis of criminal law in the UK is generally territorial, as an offence will only be triable in the jurisdiction in which it takes place unless there is a specific provision to the contrary, for instance where specific statutes enable the courts of the UK to exercise extraterritorial jurisdiction.

Some examples of exceptions are worthy of note. First, under general common law principles, if a substantial part of an offence occurs in the UK (even if other parts occur outside the UK), the UK courts can have jurisdiction.

Second, under Part I of the Criminal Justice Act 1993, certain fraud, theft, forgery, false accounting, blackmail and cheat offences are triable in England and Wales if a relevant event, or part of the wrongful act within an offence, has occurred in England or Wales. The extension of jurisdiction under this statute also applies to attempts and conspiracies to commit these defined offences.

Third, the Bribery Act 2010 (and prior bribery and corruption legislation) has important provisions to allow law enforcement to investigate and prosecute cases of overseas corruption. A feature of the extraterritorial effect of the Bribery Act is that it applies to substantive corruption offences in which the acts and omissions are entirely outside the UK, if these involve UK nationals, others ordinarily resident in the UK, or UK companies, among other defined categories of a party with a close connection to the UK. The failure to prevent an offence also applies worldwide to UK-headquartered and non-UK headquartered corporates that carry on part of their business in the UK.

In September 2018, the High Court held that section 2(3) of the Criminal Justice Act 1987, which gives the SFO power to require a person to produce specified documents in connection with an SFO investigation, has extraterritorial effect, to compel a foreign company to produce documents held outside the jurisdiction if there is a 'sufficient connection' between the company and the jurisdiction. In April 2019, the UK Supreme Court granted leave to appeal this decision.

In February 2019, the Crime (Overseas Production Orders) Act 2019 received royal assent, allowing UK law enforcement agencies to apply for a court order with extraterritorial effect (an overseas production order), to obtain data stored electronically, directly from communication service providers based outside the UK.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The challenges of dealing with cross-border investigations arise from inconsistencies in the approaches of the various law enforcement agencies and the application of different laws in the relevant jurisdictions.

The principal issues are:

- the differences in the scope and application of legal professional privilege between the jurisdictions, and ensuring that privilege is adequately protected when dealing with document or information requests from the various authorities or when conducting the internal investigation;
- the differences in data protection laws in each jurisdiction, and ensuring that breaches do not occur in the gathering and transferring of data between jurisdictions for the purposes of the internal investigation or responding to requests from a law enforcement authority;
- whether any of the jurisdictions impose a positive statutory obligation to make a formal report once the corporation becomes aware, or begins to suspect, that a crime has been committed. Northern Ireland and Scotland have additional statutes that impose reporting duties that apply in addition to laws that apply UK-wide.
- identifying which authorities may claim that the offending conduct occurred in their jurisdiction as a result of the fact that, with cloud-based communications (email, WhatsApp, i-Message, etc.), offending behaviour can occur in more than one location;
- whether evidence-sharing or mutual assistance treaties exist between the relevant jurisdictions; and
- whether there are sensitivities between the authorities in the various jurisdictions, for example, whether one authority is taking precedence, and if so whether the other authorities accept that position.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The existence of the principle of double jeopardy means that a corporation cannot be prosecuted a second time in the UK for the same or similar offences on the same facts following a legitimate acquittal or conviction, or other appropriate disposal, such as a DPA, by a UK court. European law also extends double jeopardy principles in cross-border cases within the European Union.

However, the protections for corporates worldwide in relation to double jeopardy principles are more varied and likely to be an area of discussion with law enforcement authorities when a corporate is involved in cross-border investigations in multiple jurisdictions. If the predicate offending has been disposed of in one jurisdiction, double jeopardy will not preclude UK authorities from prosecuting ancillary or incidental offences, such as record-keeping or money laundering offences that occurred in the UK. Nevertheless, there is scope to engage

with international regulators with close ties to UK enforcement agencies or mutual legal assistance arrangements with the UK (or both) to ensure that, in practice, one agency takes primary responsibility for the investigation and enforcement, to avoid any undue prejudice when a case spans multiple jurisdictions. Notwithstanding this, frequently corporates will be expected to respond to enquiries simultaneously from agencies inside and outside the UK, and there are no general, formal rights on the part of a company to seek to stay a UK investigation pending the outcome of a foreign investigation or set of criminal proceedings that may have commenced prior to the UK law enforcement agencies becoming involved.

There is no UK policy analogous to the 'anti-piling on' policy that exists in the United States. However, in situations of concurrent jurisdiction, there are memorandums of understanding between the various law enforcement and regulatory authorities in the UK. These provide a framework for co-operation between organisations that have (or may have) jurisdiction to prosecute an offence and for determining 'primacy' to investigate and prosecute offences.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global settlements have been known, such as the DPA agreed between the SFO and Standard Bank PLC in November 2015 that was coordinated with the settlement between Standard Bank and the US Securities and Exchange Commission. The SFO will also reference the assistance it receives from foreign authorities at the conclusion of any successful prosecution.

A coordinated approach between the United States and the United Kingdom was also achieved in relation to Innospec Inc and BAE Systems in 2010, although in both cases the court was critical of the coordination.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Law enforcement authorities in the UK generally try to co-operate with counterparties in foreign jurisdictions. Usually at the outset of an investigation, the authorities will agree whether one jurisdiction should take precedence in the investigation and prosecution of the matter (e.g., if the majority of the misconduct took place in that jurisdiction or in the jurisdiction of incorporation) or agree what aspect of a larger cross-border enquiry involving a corporate each will lead on if the case involves a number of components.

Even if it is agreed that the predicate offending in a matter should be prosecuted in one particular country, incidental offences, such as books and records offences, can still be prosecuted in the other jurisdictions.

Ultimately, UK authorities are responsible for the conduct of their own investigations and prosecutions. The extent to which a decision by a foreign authority would influence a UK investigation will depend on the particular facts of the matter, the relationship between the UK and foreign authorities, and the relationship between the UK and the other country on a state level, including any history of co-operation in timely mutual legal assistance.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

Currently domestic sanctions are limited to the counterterrorism regime with all other sanctions stemming from the European Union (including those implementing the sanctions imposed by the United Nations). The regulations adopted by the Council of the European Union imposing sanctions, as a tool of the EU's Common Foreign and Security Policy, are currently directly applicable in the UK.

The main types of sanctions the UK imposes are:

- trade sanctions, including restrictions relating to military and dual-use items, certain industrial sectors and the provision of certain services (these sanctions are in addition to the UK's general export control laws);
- financial sanctions, including asset freezes; and
- immigration sanctions, known as travel bans.

There may be specific exceptions under which it is possible to engage in an activity that would otherwise be prohibited. It may also be possible to get a licence or authorisation permitting activities that would otherwise be prohibited.

A principle of most sanctions regimes is the prohibition on knowingly and intentionally participating in activities that have the object or effect of circumventing any sanctions laws.

The Sanctions and Anti-Money Laundering Act 2018 will govern the sanctions regime following the UK's exit from the European Union. The UK government has been taking steps to ensure the uninterrupted application of EU sanctions post-exit, including in the case of a no-deal exit.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Although the EU regulations imposing sanctions are directly effective, UK legislation is required to introduce the penalty regimes that apply for a contravention of sanctions.

The Department for International Trade implements and enforces trade sanctions and other trade restrictions. OFSI, which is part of HM Treasury, implements and enforces financial sanctions. The Home Office implements and enforces immigration sanctions.

The potential consequences for breaching sanctions laws are severe, including unlimited criminal fines, periods of imprisonment for individuals, the disgorgement of any profits and reputational damage.

The 2017 Policing and Crime Act introduced civil penalties for breaches of financial sanctions, available in cases where it is not in the public interest to prosecute.

To date, OFSI has imposed two civil penalties: in February 2019 against Raphaels Bank and in May 2019 against Travelex (UK) Limited.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

The UK has historically had a leading role in developing the EU's sanctions policy and is embedded in a structure for co-operation on sanctions with other EU Member States.

OFSI has an international engagement branch that is leading an 'initiative to help promote robust financial sanctions implementation on the world stage, not only through bilateral and multilateral meetings/events but also through technical assistance to other governments'.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

Council Regulation (EC) No. 2271/96 protecting against the effects of the extraterritorial application of legislation adopted by a third country and actions based thereon or resulting therefrom (the Blocking Regulation) is currently directly applicable in the UK.

The Blocking Regulation currently applies to certain sanctions imposed by the United States in respect of Cuba and Iran (referred to as the listed extraterritorial sanctions). The Blocking Regulation was updated in August 2018 following the United States' withdrawal from the Joint Comprehensive Plan of Action known as the 'Iran deal'.

The Blocking Regulation has four main components:

- EU persons (currently including UK nationals and UK-incorporated entities) and those in the territory of the European Union are prohibited, without authorisation from the European Commission, from complying, either directly or through a subsidiary or other third party, actively or by deliberate omission, directly or indirectly, with any requirement or prohibition with the listed extraterritorial sanctions.
- EU persons whose economic or financial interests are directly affected by the listed extra-territorial sanctions must inform the European Commission of this within 30 days. In the case of EU businesses, the reporting obligation rests with directors, managers and others with managerial responsibility.
- Judgments or decisions of non-EU courts, tribunals or administrative authorities giving effect to the listed extraterritorial sanctions are not enforceable in the European Union. This is intended to shield EU persons, for example, from the effects of any decision requiring seizure or enforcement of any penalty in the European Union based on the listed extraterritorial sanctions.
- EU persons 'engaging in international trade and/or the movement of capital and related commercial activities between the Community and third countries' are entitled to recover damages caused to them by the application of the listed extraterritorial sanctions through the courts in Member States. Recovery can take the form of seizure and sale of the assets of the persons causing the damage, their representatives or intermediaries.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

In the UK, it is a criminal offence to breach the prohibition or fail to comply with the reporting obligation provided in the Blocking Regulation. This offence is punishable by an unlimited fine.

If a UK national or incorporated entity wishes to comply with any listed extraterritorial sanctions in the Blocking Regulation, authorisation must first be obtained from the European Commission. Applications must be made in writing to the Commission, which will consider whether sufficient evidence has been provided that the interests of the applicant or the European Union would be seriously damaged by non-compliance, based on 14 criteria set out in Commission Implementing Regulation (EU) 2018/1101. Authorisation is effective on the date when it is notified to the applicant.

To date, no UK nationals or UK-incorporated entities have been prosecuted for a breach of the Blocking Regulation.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

In addition to the normal means for identifying misconduct, such as audits, screening procedures and whistleblowing, UK companies can become aware of allegations of misconduct through cybercrime or data breaches (e.g., the *Unaoil* and *Panama Papers* cases) and due diligence carried out in relation to commercial transactions, including mergers and acquisitions.

Allegations may also arise in hearings, such as employment tribunals and litigation proceedings.

Information gathering

21 Does your country have a data protection regime?

The UK implemented the Data Protection Act 2018 (the DPA 2018) to complement the GDPR. The GDPR has direct effect across all EU Member States and applies directly to all organisations processing personal data within the European Union. However, it allows Member States limited opportunities to make provisions for how it applies in their country. The DPA 2018 essentially provides the details of local derogations, such as law enforcement processing. The two must therefore be read side by side. This new legislation supplements existing UK laws such as the Freedom of Information Act 2000 and the Regulation of Investigatory Powers Act 2000, and directly applicable EU legislation, such as the Privacy and Electronic Communications Regulations.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

In publishing its first intended fines for serious cybersecurity incidents post-GDPR, the ICO has demonstrated its intention to use the full force of its powers. In July 2019, the ICO reported its intention to fine British Airways £183.39 million in relation to a cyber incident involving the compromise of personal details of around 500,000 customers; similarly with the ICO's reported intention to fine Marriott International, Inc more than £99.2 million in relation to a cyber incident whereby the records of approximately 339 million guests globally were exposed.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

Typically, a considerable amount of evidence will be reviewed in the course of any internal investigation and must be handled carefully to ensure compliance with the DPA 2018. It is very likely that it will be necessary to conduct a data privacy impact assessment before processing any information. Decisions taken with regard to the processing and disclosure of data should be made in accordance with the DPA 2018, and all reasons for those decisions should be documented. If any of the data reviewed contains or may contain personal data, particularly sensitive personal data, extra care should be taken. Firms should seek legal advice with regard to what additional measures should be taken in relation to this material. This includes whether redaction of any personal information is required and whether this would be an appropriate mechanism to avoid any data protection breaches.

Further, extra care should be taken in circumstances where there may be a transfer of the data outside the European Union or a jurisdiction with an adequacy decision (i.e., a jurisdiction that offers an equivalent level of protection to data as in the European Union).

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

A range of factors must be taken into account when considering the monitoring of employee communications. These typically fall into two categories:

- review of emails sent and received by an employee; and
- intercepting emails before receipt.

In relation to the review of emails sent and received by an employee, the situation broadly involves considerations under the GDPR, the DPA 2018 and the Human Rights Act 2000. The processing of emails through review will require an employer to consider the extent to which it can satisfy a lawful condition of processing under the GDPR with balancing the data subject and privacy rights. However, consent is not typically a basis upon which such processing would take place as consent, under the GDPR, has to be freely given and the ICO has stated that it is unlikely that consent could be so considered in an employer–employee relationship in view of the imbalance of power.

If monitoring does take place, this will often be overt monitoring, in that the employer will set out in its information technology (IT) use and privacy policies that they retain the right to access emails and messages sent and received on employer-issued devices.

The ICO issued guidance prior to the implementation of the GDPR that, at the time of writing, has not been updated but recommends that covert monitoring only takes place in exceptional circumstances; for example, for the detection of crime.

It is essential, if monitoring is taking place, that the employer ensures that it is proportionate and undertaken only for as long as is necessary.

The GDPR sets out circumstances in which it is mandatory to conduct a data protection impact assessment, which includes assessing when processing is likely to result in a high risk to data subjects. As a matter of good practice, it may be prudent to work through a risk assessment prior to processing even when the high threshold has not been triggered, so that essential security and data minimisation measures are considered and adopted where necessary.

Up to 27 June 2018, the Provisions of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699) governed the interception of electronic communications during transmission. Since that date, these have been replaced by the Investigatory Powers Act 2016 (IPA) and the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (S 2018/356) (the 2018 Regulations).

Under the IPA, it is a criminal offence to intercept communications without lawful authority. Although the 2018 Regulations include the detection of crime as authorised conduct in certain circumstances, given the criminal implications of interception without proper authority, every case must be assessed on its merits to ensure that the relevant standards are met.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Authorities that investigate corporate crime in the UK, such as the SFO, often conduct dawn raids of business or residential premises under the authority of a search warrant issued by a court. Depending on the specific powers of the law enforcement agency conducting a raid, the raid is often undertaken in coordination with a local police force.

When a raid is carried out under a warrant, the authority may only search the premises specified in the warrant and seize items within the scope of the warrant.

In England, Wales and Northern Ireland, certain categories of material, such as confidential journalistic material or personal records created in the course of a business (e.g., patient records in a medical practice) cannot be seized during a raid without additional authorisations being obtained, in some circumstances from particular courts. Different rules apply in Scotland.

In the UK as a whole, legally privileged material cannot be seized unless it was created with the intention of the furtherance of a crime (crime-fraud exception) or is inextricably linked to other, seizable material. In that case, it can be seized but must be sifted to exclude as far as possible any privileged material from the investigating team at the law enforcement agency. In England and Wales, a typical approach is for material subject to a claim of legal privilege to be examined by an independent lawyer before it is examined by the investigating team (and any privilege material excluded). The use of this power is also subject to the Criminal Justice and Police Act 2001, which entitles a corporate's legal representative to be present at a review of the material and apply to a judge for the material to be returned. In Scotland, there is no statutory framework for dealing with privilege issues and there may be a need to apply to the courts for the seizure of privilege material to be suspended.

The CMA may conduct a dawn raid of business premises without a warrant.

Some authorities have additional powers that can be exercised during a dawn raid, for example, the SFO and the CMA may compel a person to answer questions relevant to the search, such as regarding the location of certain documents.

If there are significant errors in either the process of obtaining a warrant or authorising a raid, or in the execution of a raid, the raid can be challenged by judicial review and rendered unlawful and the material seized during the raid could be rendered inadmissible.

The Law Commission is reviewing the law governing search warrants. A consultation on the issue closed on 5 September 2018. The Commission's report and recommendations are still awaited.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

As a general rule, legally privileged material cannot be seized during a dawn raid unless the crime-fraud exception applies or where it is inextricably linked to seizable material (as described in question 25), in which case other safeguards, including those set out in question 25, should be adhered to. However, in relation to certain competition investigations, the European Commission does not regard advice from in-house lawyers as legally privileged, so it may seize such material during raids or inspections.

In England, Wales and Northern Ireland, the authorities that investigate corporate crime are routinely accompanied during raids by an independent lawyer specifically tasked with reviewing on-site any material that a company asserts as privileged. It is, therefore, important to be aware of where privileged material is likely to exist so that assertions can be made before items are seized.

If there is a dispute regarding privilege, the authority will seize the material by sealing it in an opaque bag for review by an independent lawyer at a later date. The company is entitled to have its legal representative present during that review.

Digital devices containing both privileged and non-privileged items that cannot be separated may be seized or imaged during a raid. In practice, the privileged material will then be quarantined by digital forensic experts within the authority by applying search criteria provided by the company.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

In England, Wales and Northern Ireland, there is a qualified right of silence when being interviewed as a suspect, and a defendant in a criminal trial has a right not to give evidence. In both situations, the right is qualified as, in certain circumstances, adverse inferences can be drawn from this silence.

However, in Scotland the right to silence is not qualified and no negative inference can be drawn from an interviewee's refusal to answer questions.

A right of silence does not apply when an authority such as the SFO, FCA or CMA exercises specific statutory powers by issuing a notice compelling a witness to answer questions or produce documents. Failure to comply with such a notice without a reasonable excuse can result in a criminal offence. However, the contents of a compulsory interview under these powers cannot be used against the individual except in a prosecution specifically for making a false or misleading statement in that interview. In practice, complications can arise when an individual is initially a witness compelled to produce evidence and then later becomes

a suspect in a criminal investigation. Any evidence provided in the subsequent interviews conducted under caution can be adduced against the individual.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The Public Interest Disclosure Act 1998 and the Public Interest Disclosure (Northern Ireland) Order 1998, as amended, combined with the Employment Rights Act 1996 and the Employment Rights (Northern Ireland) Order 1996, offer statutory protections to whistleblowers.

The dismissal of an employee will be automatically unfair if the principal reason for dismissal is that the individual has made a qualifying 'protected disclosure'. Workers and employee are also protected from detrimental treatment (e.g., harassment, reduction in pay or dismissal) on the ground that they have made a qualifying protected disclosure.

There is no requirement for a minimum period of service nor is there any financial cap on the amount of compensation that can be awarded. An employee alleging automatic unfair dismissal on the grounds of being a whistleblower may make an immediate application for interim relief which may result in effective reinstatement. A successful automatic unfair dismissal claim could also result in the individual being reinstated as an employee, although this is rare.

There are no financial incentive schemes in the UK for whistleblowers.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Suspension pending investigation

Employment legislation does not specifically deal with suspension but case law and guidance issued by the Advisory, Conciliation and Arbitration Service (ACAS, a public body funded by the UK government), in the form of the ACAS Code of Practice on Disciplinary and Grievance Procedures (the ACAS Code), requires that employees only be suspended where this is necessary and that the period of suspension be as short as possible. It is also important that employees be informed, preferably in writing, of the nature of the allegations made against them (whether in relation to an internal or external investigation) and, in most cases, suspension should be on full pay and with no loss of benefits. Any failure to follow these principles can result in a breach of the ACAS Code and a repudiatory breach of contract. In Northern Ireland, similar provisions apply, pursuant to the Labour Relations Agency, Code of Practice on Disciplinary and Grievance Procedures (the LRA Code).

The right to a fair hearing

The disciplinary process should be carried out in accordance with the ACAS Code. As a minimum, it should include an investigation to establish the facts before proceeding to a disciplinary hearing (assuming there is a case to answer). In good time ahead of a disciplinary

hearing, the employee must be informed of the allegations against him or her and the right to be accompanied at the hearing by a colleague or a trade union representative. During the hearing, the accused should be given a full opportunity to answer the allegations before any decision is made by the employer.

Employers should carry out their own disciplinary process irrespective of any third party finding of guilt (e.g., the police). The employer is still required to follow a fair disciplinary process (in accordance with the ACAS Code) as far as possible. As stated above, in Northern Ireland, compliance with the LRA Code (rather than the ACAS Code) is required but also note that, unlike in Great Britain, statutory dismissal procedures have been retained.

These requirements can be relaxed when employees do not have the requisite length of service with their employer to bring an unfair dismissal claim (two years in Great Britain and one year in Northern Ireland); however, it is best practice to follow a fair process in dismissals, to avoid allegations of whistleblowing or discriminatory treatment.

The right not to be unfairly dismissed

All employees with the requisite length of service have the right not to be unfairly dismissed. In the case of a successful claim, an employment tribunal can order reinstatement or re-engagement, or award compensation. In most cases in Great Britain, compensation is capped at one year's pay or £86,444 (whichever is lower) plus a basic award of up to £15,750. In Northern Ireland, the one-year pay cap does not apply and unfair dismissal compensation is capped at £86,614, plus a basic award of up to £16,410, although in certain situations, employees can argue that this compensation cap should be disapplied.

The requirement for length of service and the statutory caps on compensation do not apply where the employee successfully alleges that the principal reason for dismissal is that the individual made a qualifying protected disclosure.

Company director considerations

Directors may also be employees (in which case the above will apply in tandem with any specific issues regarding directors' duties). A director who is not an employee (a non-executive director) will not be subject to the above rules. However, directors are subject to general duties, which are set out in the Companies Act 2006, contained within a company's articles and may also be set out in any letter of appointment. The company's articles and any relevant letter of appointment will include provisions regarding the removal of a director who has acted in breach of one or more of his or her duties under the Companies Act. There are additional regulations that apply to directors of public companies.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Rights regarding suspension, the right to a fair hearing and the right not to be unfairly dismissed all apply to employees who may have engaged in misconduct. In general, there is no strict employment law requirement to suspend or discipline those suspected of misconduct; that is a decision for the employer. Some heavily regulated employers, such as those

within the financial services sector, may be required by their regulatory body to suspend and take disciplinary action against employees who carry out regulated activities. In some cases, an employee's misconduct must be reported to the regulator. Employees may also be regulated themselves and will have specific obligations towards the regulator.

Failure to take disciplinary action could be regarded by an authority as evidence of poor corporate culture. Furthermore, failure to suspend or dismiss an employee who is capable of impeding a criminal investigation by destroying documents or alerting or interfering with witnesses, could be regarded as obstruction of the criminal investigation.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

In general, a request to participate in an internal investigation will be a reasonable management instruction and any unreasonable refusal to engage in this process may constitute misconduct in itself. Whether or not an employer could fairly dismiss in these circumstances will depend upon the whole context and in particular the seniority of the employee. At all times, it is important that the employer does not interrogate or put pressure on the employee to make admissions of guilt, and a range of safeguards as to how the investigation is conducted should be considered, to ensure fairness to the employee.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is good practice to prepare an initial scope of an internal investigation, potentially with a written investigation plan, with target deadlines and a clear set of tasks where possible, before commencing the investigation proper, setting out:

- its purpose;
- the issues to be investigated;
- the investigation team and reporting lines;
- how legal privilege will be established and maintained (e.g., the investigation team is instructed by and reports to a lawyer);
- how digital and hard copy material will be collected and preserved;
- how staff interviews will be conducted; and
- any other necessary immediate controls or steps, such as ceasing all future payments to suspect third parties.

The scope of an internal investigation and the client team may need to be kept under review, depending on factual findings and other developments that are possible at different stages in the investigation.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

In UK law, there are generally no formal legal obligations on a company to conduct an internal investigation into its own affairs. However, conduct rules applicable to some companies by the bodies that regulate them may mean an internal investigation is strongly recommended or even required. Generally, from an effective compliance perspective, a company should always investigate an issue as soon as it comes to light to enable the company to take the steps set out below (see also question 36).

The company will also need to consider whether a money laundering report is needed in accordance with the Proceeds of Crime Act 2002 (UK-wide application) and whether any additional report is required for the police in Northern Ireland or Scotland to comply with specific legislation that is applicable in those jurisdictions. In addition, the company should:

- stop the offending behaviour, otherwise the company could be exposed to a risk of criminal liability itself for allowing potential offending to carry on unchecked and uninvestigated. Additionally, if the offending conduct has ceased and the company is aware or suspects that it possesses funds obtained from the conduct, but it fails to take any action in regard to those funds, for example making a suspicious activity report to the NCA, the company could commit a further money laundering offence;
- preserve all documents and material relevant to the issue. If a law enforcement authority becomes aware of the matter, it would expect the company to have taken all necessary steps to protect and preserve all material that would be relevant to its criminal investigation (including by taking forensic images of digital material) so that the material could be provided to them eventually. Failure to do so could impede a criminal investigation and would be viewed as a lack of co-operation by an authority. Furthermore, it can be a criminal offence to destroy, falsify, conceal or dispose of relevant documents when a person knows or suspects an investigation of serious or complex fraud is already being, or is likely to be, undertaken by certain law enforcement agencies.
- take remedial or preventive action to ensure that the offending behaviour cannot occur in the company again.

If a company has failed to take any steps to address an allegation of bribery, it is unlikely that it would be able to rely upon the 'adequate procedures' defence in the event of a prosecution of corporate failure to prevent bribery under the Bribery Act 2010.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Upon receipt, the notice or court order should be sent immediately to the appropriate person within the business, whose function is to deal with such external matters (usually within the legal department). All steps should be taken to ensure that evidence that may be relevant for production under the notice or court order is not deliberately or inadvertently lost, destroyed or altered, and that any individuals who may be involved in possible wrongdoing are not tipped off. The exact scope of the request should be determined, and clarifications sought if

the scope is unclear. The deadline for responding should also be diarised. It is advisable to seek external legal advice if the legal department is inexperienced in dealing with such matters.

To the extent that a company has an internal policy setting out the steps to be taken upon receipt of a notice or court order, this should be followed. Among other steps, the company should consider circulating document retention notices to ensure all relevant data is preserved, taking forensic images of all potentially relevant data sources (e.g., laptops, PCs, tablets, phones), and compiling a database that can be interrogated for documents falling within the request.

Once reviewed for relevance, the results should be double-checked for privilege and copies retained of anything provided to the authorities.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

Privately owned companies are not required to publicly disclose the existence of internal investigations or contact from law enforcement.

Under the UK Listing Rules, publicly listed companies must issue a market announcement of any major new development that may affect their business without delay, if the development may lead to a substantial share price movement. A notice compelling the provision of documents would be unlikely to require an announcement, but confirmation from the authority that the company was a suspect in a criminal investigation would be likely to require an announcement.

Organisations that are authorised by the FCA also have an obligation to disclose to it anything relating to the firm of which it would reasonably expect notice. This would include breaches of UK laws and regulations, civil, criminal or disciplinary proceedings against a firm and fraud, errors and other irregularities.

36 How are internal investigations viewed by local enforcement bodies in your country?

UK authorities have publicly stated that they are not opposed to internal investigations that are carried out in a manner that would not impede a criminal prosecution. They expect data gathering exercises to be carried out promptly, covertly and coordinated across multiple sites simultaneously. 'Covert' in this context is intended to ensure potential suspects in a later criminal investigation are not tipped off prior to data collection and so given an opportunity to destroy or delete incriminating material. It does not mean that companies should conduct internal investigations in a manner that involves unlawful surveillance or data gathering techniques (whereby they could be separately liable for other offences). In practice, digital material should be forensically imaged and preserved by IT specialists. All procedures used to gather and image data should be recorded and then fully disclosed to the relevant law enforcement authority.

Additionally, UK authorities expect that full and accurate accounts are taken during any witness interviews and, in some circumstances, consideration may need to be given to whether certain interviews should be conducted at all. This is particularly important if there is a risk of criticism that a corporate conducted an interview knowing a law enforcement

agency would wish to speak to a witness first and obtain a first account from a witness prior to any internal investigation or review.

The SFO has repeatedly said that it expects to be given interview notes by corporates seeking to demonstrate co-operation in their investigation. While this is tempered to an extent by an acknowledgement that disclosure is not required when legal professional privilege applies, where such a claim is without foundation, co-operation is likely to be cast into doubt in the absence of such disclosure.

Prior to the Court of Appeal decision in September 2018 in *SFO v. ENRC*, provision of interview notes would normally be expected by the SFO in the event of any self-report by a corporate, and any claims of privilege over those accounts were uncertain (and likely to be contested by the SFO).

Following *ENRC*, there are now more established grounds for litigation privilege to apply to interview notes, depending on the factual context of an internal investigation (see further at question 37).

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Legal professional privilege has traditionally been claimed over various aspects of internal investigations, which, in recent years, has increasingly been disputed by law enforcement authorities. However, in a 2018 Court of Appeal case, Eurasian Natural Resources Corporation Limited (ENRC) successfully repelled a challenge by the SFO relating to claims of privilege by ENRC. The SFO sought to challenge claims to privilege by ENRC regarding various documents that were produced by lawyers and forensic accountants during an internal investigation into allegations of bribery and corruption that had arisen from a whistleblower report. The documents in question fell into four categories:

- category 1: notes taken by lawyers of interviews conducted during an internal investigation;
- category 2: materials generated by forensic accountants as part of a 'books and records' review;
- category 3: documents, such as a presentation slides, containing or surmising factual evidence, that were used by lawyers to present to ENRC; and
- category 4: emails between a senior executive and the head of mergers and acquisitions at ENRC, who was a Swiss qualified lawyer.

The Court of Appeal held that documents falling into categories 1, 2 and 4 were protected by litigation privilege. The High Court had already held that the factual updates provided in category 3 were protected by legal advice privilege.

In short, the Court of Appeal held that a criminal investigation by the SFO could be 'litigation' for privilege purposes and that while a party anticipating possible prosecution will often need to make further investigations before it can say with certainty that proceedings are likely, that uncertainty does not in itself prevent proceedings being in reasonable contemplation. The fact that ENRC did not have the information required to evaluate the whistleblower email, therefore causing it to be uncertain as to whether a crime had in fact taken

place, was not a bar to having the protection of litigation privilege. The Court opined that it would be wrong to deny a potential defendant the benefit of litigation privilege when he or she asks his or her lawyer to investigate the circumstances of the alleged offence. It concluded that ENRC did contemplate that prosecution was possible when the documents in question were created and these documents were therefore protected by litigation privilege. Much of the reasoning of the Court of Appeal decision is highly fact specific in the circumstances of the *ENRC* case. Therefore, the judgment should not be interpreted to extend litigation privilege to all documents created in all internal investigations.

While the question of whether or not privilege will apply remains fact specific, there are nevertheless several standard ways to advance and strengthen any legitimate claim to privilege, such as:

- involving lawyers (whether external or internal) as soon possible;
- marking all communications pertaining to legal advice as 'privileged and confidential';
- segregating privileged and non-privileged documents;
- refraining from forwarding or creating new documents that summarise legal advice received;
- encouraging employees not to amend or quote extracts from legal advice;
- where there is the reasonable possibility of potential litigation at a later stage, recording this in writing when the future possibility arises in an internal investigation, to evidence any subsequent legitimate claim for litigation privilege; and
- only circulating legal advice and privileged material on a strictly need-to-know basis.

Parties are able to obtain legal advice in the context of an internal investigation, and communications between a lawyer and a client for the purposes of legal advice continue to be privileged under legal advice privilege principles. These principles generally do not protect communications involving third parties. However, the Court of Appeal in *ENRC* has expressly left open a question as to whether aspects of current UK law on legal advice privilege (see the *Bank of England BIU* case) should be reviewed at a later date by the UK Supreme Court. It is therefore likely that the subject of privilege in internal investigations will be a matter of ongoing development of UK law.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

There are two main forms of legal professional privilege in the UK: (1) legal advice privilege, which protects confidential communications (and evidence of those communications) between a lawyer and a client (but not communications with third parties) provided that the communications are for the dominant purpose of seeking and receiving legal advice; and (2) litigation privilege, which protects confidential communications (and evidence of those communications) between a lawyer and a client or third party, or both, or between a client and a third party, created for the sole or dominant purpose of obtaining information or advice in connection with the conduct of existing or reasonably contemplated litigation (including avoiding or settling, as well as defending or resisting, that litigation).

The holder of the privilege is the client.

In the case of corporate investigations, the client tends to be represented by the group of individual employees or directors charged with seeking and receiving legal advice on behalf

of the company (or commissioning or conducting the internal investigation) rather than the entire corporate entity. This group of individuals usually includes the in-house legal team and some or all of the board of directors or subcommittee established by a company, but this group should be defined as soon as any external lawyers are engaged or at the outset of an investigation. This helps to ensure that there is a defined group from whom instructions by lawyers can be received and to whom advice is provided, which safeguards any claim of legal advice privilege.

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes, although not in the context of an antitrust and competition investigation by the European Commission. In-house counsel must always be careful to ensure that they distinguish between legal advice and advice that is commercial in nature, since the latter will not attract legal professional privilege.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

Advice sought from foreign lawyers in investigations in the UK is subject to the same legal professional privilege as advice sought from lawyers within the UK. The UK courts will apply UK law on privilege to determine the extent to which privilege applies. If a document satisfies the test for legal advice privilege or litigation privilege under UK law, the document will be treated as privileged. This decision is made regardless of whether that document would not have been privileged under a foreign law.

This principle can have the opposite effect in respect of any documents that would be privileged under foreign law but do not meet the requirements for privilege under UK law. Such foreign privileged documents would not attract legal professional privilege in the UK.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

UK authorities have frequently stated that they have no interest in communications between a client and its lawyers as to questions of liability or rights; however, in recent years, law enforcement agencies such as the SFO have challenged assertions of legal professional privilege over factual aspects of internal investigations and have expected the waiver of claimed legal professional privilege in the event of any self-report.

The authorities have stated previously that a refusal to waive a well made-out claim of legal professional privilege will not be held against a company, but a waiver of such a claim would be good evidence of co-operation. False or exaggerated claims of legal professional privilege will continue to be considered strong evidence of not co-operating and will be challenged.

The 2018 *ENRC* Court of Appeal judgment has confirmed that even when a party may lead the SFO to believe that it might in future waive privilege over certain documents, this does not in itself amount to a waiver of privilege and would only amount to such a waiver in the event of a formal agreement.

In summer 2019, the SFO issued some long-awaited guidance on its requirements for a company to be considered to be adopting a co-operative approach with the SFO in relation to allegations of fraud, bribery, money laundering and a failure to prevent the facilitation of tax evasion, which will influence its charging decisions. Other regulators may refer to the guidance in assessing whether the subject of an investigation has co-operated. In relation to legal professional privilege, the guidance provides that 'if the organisation claims privilege, it will be expected to provide certification by independent counsel that the material in question is privileged'.

With regard to witness accounts collated in the course of internal investigations (presumably prior to reaching a conclusion that there was a potential corporate offence that should be notified to the SFO), companies are expected to provide those witness accounts to the SFO as a mark of co-operation.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

There is a concept of limited waiver of legal professional privilege, and it is for the individual or entity waiving the privilege to determine the extent of the waiver.

It is important to be very clear as to the scope of the waiver with regard to the purpose for which the privileged information can be used and with whom it can be shared, particularly if a party seeks to prevent the information being shared with other domestic or foreign enforcement authorities or parties in any related civil proceedings. Generally, there are various gateways where evidence is shared between law enforcement agencies in the UK (and sometimes elsewhere), and proposals for a limited waiver from a corporate may not be acceptable to a law enforcement agency given the wider duties of disclosure or information-sharing.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

This will depend on a number of factors, including the terms of the waiver, the circumstances in which the material was received by the UK authority, and whether the UK authority disputes the claim of privilege, for example, if the UK authority asserts that the material falls within the crime-fraud exception.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege exists in the UK and can be used to preserve privilege in documents disclosed to third parties who have, at the time of the disclosure, a common interest in the subject matter of the privileged document or the litigation for which the document was created.

It is advisable when disclosing information under the common interest privilege to ensure that the recipient understands that the document has been disclosed on this basis and to obtain undertakings from the recipient that the privilege will not be waived. Typically, in criminal-related investigations, common interest privilege has very limited practical scope, because it is often in doubt whether two parties do, in fact, have a common interest.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

Privilege can be claimed over confidential communications (and evidence of those communications) between a lawyer and a client or third party, or both, or between a client and a third party, created for the sole or dominant purpose of obtaining information or advice in connection with the conduct of existing or reasonably contemplated litigation (including avoiding or settling, as well as defending or resisting, that litigation).

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

An internal investigation is a fact-finding exercise and interviews will often be central to any internal investigation. However, it is advisable always to be sensitive to the expectations of investigating authorities, to avoid any criticism that such interviews could have prejudiced the law enforcement investigation.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

While privilege is often claimed over internal witness interviews, UK authorities, such as the SFO, have stated in the past that they do not accept that the factual accounts of a witness interview are privileged and disapprove of such claims. This culminated in an unsuccessful challenge by the SFO over materials produced during an internal investigation on behalf of ENRC (see question 37), in which the Court of Appeal held that factual notes of what is said by a witness to a lawyer constituted a privileged document on the particular facts of the *ENRC* case.

It should also be borne in mind that in situations where proceedings are not in contemplation, communications between interviewees and counsel not made in the course of giving instructions to counsel will not attract litigation privilege or legal advice privilege. Only communications between counsel and those entrusted by the company to give instructions to counsel will attract legal advice privilege.

As stated under question 41, in summer 2019, the SFO issued some long-awaited guidance on its requirements for a company to be considered to be adopting a co-operative approach with the SFO, which includes guidance on witness interviews.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Although there are no general, formal requirements when conducting witness interviews as part of an internal investigation, best practice dictates that, irrespective of whether the interviewee is an employee or a third party, they should be informed:

- that the interview is part of a fact-finding exercise and, if applicable, in contemplation of litigation;
- if they are implicated in any wrongdoing;

- that the lawyer conducting the interview represents the company and not the interviewee;
- that the interview notes created by the lawyer belong to the company and therefore any privilege in the notes rests with the company;
- the company may choose to provide the notes to an authority (and this is at its election); and
- that the interview is confidential and the contents of the interview should not be discussed with other employees or witnesses (to avoid contaminating their recollection and generally to protect the integrity of the process).

Care should also be taken not to taint the witness's recollection, for example by disclosing previously unseen material or discussing another witness's statement.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

It is common for interviewees not to be legally represented in initial fact-finding interviews during internal investigations; however, companies should not refuse a request from an individual to be legally represented at his or her own expense. In other circumstances, for example where an employee may incriminate himself or herself during an interview, there are compelling ethical reasons why a company may suggest that an employee may wish to obtain his or her own independent legal advice.

Documents can be put to the interviewee. A copy of each of the documents referred to or an interview pack should be retained as part of the record of the interview, as a matter of good internal investigation practice.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

The Proceeds of Crime Act 2002 (POCA) places a specific duty on employees of regulated businesses (i.e., financial services firms and professional services such as lawyers and accountants) to make a report to the NCA when they have reasonable grounds to know or suspect that another person is engaged in money laundering and that knowledge came to them within the course of their regulated business. Failure to make a report in those circumstances carries a risk of imprisonment or a fine, or both, for individuals (and fines for companies), unless, in the case of individuals, they have reported to their firm's money laundering reporting officer (MLRO). Other similar offences arise in the case of MLROs who have failed to report to the NCA, given their designated statutory duties to do so.

All companies (regulated and non-regulated) should make a report to the NCA if the company has a suspicion that it possesses funds obtained as a result of suspected criminal conduct by the company or employees, as this may be a money laundering offence under POCA. Other offences can arise if transactions involve the facilitation of money laundering offences by other persons. A report to the NCA of any of these types of suspicions can provide a statutory defence to money laundering if made as soon as practicable.

A money laundering report to the NCA is not a self-report for the purposes of a DPA (see question 51) or mitigation of sentence. A self-report must be made directly to the relevant authority, such as the SFO.

In Scotland, there is an obligation to report any knowledge or suspicion of serious organised crime to the police when this knowledge or suspicion originates from information obtained in the course of business or as a result of a close personal relationship (Criminal Justice and Licensing (Scotland) Act 2010). In Northern Ireland, additional reporting duties apply under the Criminal Law (Northern Ireland) Act 1967.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

The question of when and whether to self-report in the UK has been the subject of considerable debate following the *Rolls-Royce* case, which involved a DPA, notwithstanding that there was no self-report by Rolls-Royce.

A DPA is an agreement reached between a prosecutor and a company under investigation and approved by a court. The agreement allows a prosecution to be suspended for a defined period provided the organisation meets certain specified conditions. If the conditions are met, the prosecution is formally discontinued. (For further information about the DPA process in the UK, see question 65.) Prior to the DPA agreed in *Rolls-Royce* in January 2017, it was considered advisable for a company to self-report if it wished a matter to be settled by way of a DPA; the SFO had articulated that one of the preconditions of a DPA was a genuinely proactive approach by the company, including a full self-report (i.e., complete disclosure of the facts).

However, the stance that a self-report was a precondition to a DPA was put into some doubt in light of the DPA secured by Rolls-Royce in circumstances that did not follow a self-report. The SFO, and indeed the court in approving the DPA, has emphasised that the circumstances in which Rolls-Royce secured a DPA, notwithstanding that it had not self-reported, were due to the extraordinary level of co-operation with the SFO that followed once the offending conduct was already in part known to law enforcement authorities. The 'extraordinary co-operation' that was commended in the court's judgment included a comprehensive internal investigation that extended beyond the original allegations known to the SFO, the results of which were made available to the SFO; disclosure of unreviewed documents; access to witnesses who had not previously undergone interviews by the company; and a limited waiver of any claim for legal privilege – all of which, the judgment suggests, brought to light conduct that otherwise may not have been exposed.

As stated in question 41, the SFO has now issued guidance on what it considers amounts to co-operation with its investigations, including a requirement to report a suspected fraud or bribery within a reasonable time of the suspicion arising. The guidance makes it clear that co-operation will be a relevant factor in making charging decisions (i.e., whether to prosecute, recommend a DPA or take no further action). There is no presumption that self-reporting will lead to no further action.

The SFO does not publish details of the self-reports that have led to no further action. Whether a DPA will be available in the absence of a self-report in future remains to be seen, but the benefits of so doing were highlighted recently in a case brought by the SFO against

company director Carole Ann Hodson. The new company owners became suspicious and reported their concerns to the SFO, which launched an investigation into the company, its officers, employees, agents and associates. Hodson was then prosecuted and convicted. No action has been taken against the company – a reminder of the potential benefit of self-reporting by companies in appropriate cases, when the public interest may be served by taking action against the former owners and wrongdoers, rather than the company itself.

The question of when, and indeed whether, to self-report came into sharp focus again in relation to the Tesco Stores Limited DPA and subsequent acquittal of its senior executives. After discovering issues in the executives' financial statements, Tesco referred itself to enforcement authorities. On 10 April 2017, Tesco entered into a DPA in respect of false accounting charges. This decision has subsequently been called into question by some following the collapse of the trial of two Tesco executives accused of the same false accounting. The judge concluded that the SFO's evidence, taken at its highest, was such that a jury could not properly convict. The SFO subsequently offered no evidence at the trial of a third director.

A charge of accounting fraud, however, requires the conviction of a senior executive, or 'directing mind and will', to bind the guilt of the company. In short, the company cannot be guilty without the guilt of the senior executive. This contrasts with the corporate offence of 'failure to prevent bribery' under the Bribery Act, which does not depend on the guilty mind of a senior executive. If a company pleads guilty to a fraud offence, such as accounting fraud, at an early stage and secures a DPA, there is a risk that a jury, on consideration of the complete evidence at a later stage, will not be satisfied beyond reasonable doubt that the relevant individual is guilty. Therefore, companies must carefully assess the evidence against them before entering into a DPA. In cases that do not involve a 'failure to prevent' offence, the company may be hesitant to enter into a DPA given the difficulties of prosecuting these offences. The importance of making the correct decision is reinforced by the expense of a DPA and the requirements of extensive co-operation with the SFO.

DPAs are only available to corporate defendants and not to the individual employees or directors involved in the criminal conduct.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

Before making a self-report, a company should undertake the appropriate level of investigation to ascertain the extent and nature of the offending, ensuring that the company will not be taken by surprise by further issues that could arise in the course of a criminal investigation.

UK authorities have advised that for a company to be afforded full credit for making a self-report, it must be made within the context of a genuinely proactive and co-operative approach by the company. The SFO's Corporate Co-operation Guidance sets out the steps it expects an organisation to take to demonstrate such co-operation.

The SFO's outline of the process to be adopted by corporate bodies or their advisers when self-reporting provides that:

- initial contact, and all subsequent communication, must be made through the SFO's Intelligence Unit, using the secure reporting form;
- hard copy reports setting out the nature and scope of any internal investigation must be provided to the SFO's Intelligence Unit;

- all supporting evidence, including, but not limited to, emails, banking evidence and witness accounts, must be provided to the SFO's Intelligence Unit; and
- further supporting evidence may be provided during the course of any ongoing internal investigation.

In Scotland, the COPFS's self-reporting policy, which applies in relation to corporate bribery offences, requires a written report to be submitted on the company's behalf by a solicitor.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

It is both possible and desirable to enter into a dialogue with the authority before or upon receipt of a notice or warrant to discuss any concerns the company has, for example that the deadline for compliance is unreasonable, or the description of the information and documents requested is unclear.

The authority should be willing to discuss such concerns and work with the company to find a reasonable and practical solution, so long as the result is that the relevant information and documents are ultimately received in a timely fashion. With regard to search warrants served on businesses, the police do not usually contact a business to discuss the terms of a warrant prior to turning up and executing the warrant. However, depending on the circumstances, the police may be willing to discuss the implementation of the warrant to avoid unnecessary disruption to the business's legitimate activities and the risk of the warrant being challenged.

Materials subject to legal professional privilege may be withheld when responding to a search warrant. Warrants often do not address how privileged materials should be handled, and dealing with issues of privilege tends to be a matter for negotiation. The legal agent for the company should object to privileged materials being reviewed or seized and offer to set aside potentially privileged materials for review by the company's legal agent subsequently. If the authority will not agree to this course, it may be proposed to appoint independent counsel (usually an advocate, barrister or solicitor) to review potentially privileged material and to make a determination as to whether or not the material is, in fact, privileged. If the authority will not agree to proceed on that basis, the legal agent for the company should insist that any privileged material should be sealed, unread, and delivered to the court to enable it to adjudicate upon the matter. In the event that such suggestions are not acted upon by the authority, the company may need to seek to overturn the warrant by presenting to the court a judicial review (or a bill of suspension in Scotland). (See also question 26.)

54 Are ongoing authority investigations subject to challenge before the courts?

The exercise of powers by any public authority, such as in undertaking an investigation, can be challenged by application to the court for a judicial review (a bill of suspension in Scotland) if considered to be unlawful.

If found to be unlawful, the court can order various remedies, such as stopping the exercise of that power, rendering it ineffective or awarding damages.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

While attempting to deal with notices or court orders issued by various jurisdictions as one consistent disclosure package would reduce effort and costs, it is generally advisable to deal with them separately but have protocols in place to ensure consistent approaches are maintained to any relevant documents to be produced. Court orders and notices issued under compulsory powers usually negate data protection laws and any obligations of confidentiality to third parties. Consequently, civil proceedings cannot be brought by third parties against a company for its actions in providing material in response to a lawful court order or compulsory notice as long as the material provided was within the scope of the notice or order. However, if the company voluntarily provides material beyond the scope of the notice or order, and in doing so breaches a confidentiality obligation or data protection law, it could expose itself to claims.

To avoid creating risks of civil and criminal liability, notices and orders should be responded to separately unless the company is able to satisfy itself that the scope of the orders or notices from each of the jurisdictions are identical in all important respects.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

In general, if information is in the control of a company (e.g., a parent company with a right to take possession, inspect or take copies of a subsidiary's documents), the company will be expected, and may be required, to search for and produce all requested material, even when it is located in another country. In practice, if the company wishes to seek credit for co-operation, it should comply with any reasonable requests, whether or not it is required to. Also see question 10.

The exception is when the data protection legislation in the other country does not permit the removal or transfer of the data from that jurisdiction. In those cases, the requesting authority will generally need to use mutual legal assistance to obtain the material through foreign counterparts.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

The UK authorities can and do share information and investigative materials with authorities in various other countries (for intelligence purposes and the detection and prevention of crime), whether or not there is a mutual legal assistance agreement with that country. This occurs regardless of whether the country is providing information or materials in return, although reciprocity is generally expected.

Where material is required for a prosecution, a mutual legal assistance request must be made. UK law authorities will only provide assistance that conforms with the UK's laws and international obligations.

A list of the international mutual legal assistance and extradition agreements to which the UK is a party can be found on the UK government website (www.gov.uk/government/publications/international-mutual-legal-assistance-agreements).

The UK authorities can provide further assistance by conducting dawn raids in the UK on the foreign authority's behalf, interviewing witnesses or suspects, freezing assets, or arresting and extraditing suspects.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Law enforcement authorities owe a general duty not to disclose information or material received during the course of an investigation, and which is not otherwise in the public domain, unless the public interest in the disclosure outweighs the private interests of the owner. Furthermore, before disclosing information to a third party, the law enforcement agency should provide the owner with sufficient notice of the request to allow an opportunity for objections to the disclosure (*Marcel and Others v. Commissioner of Police of the Metropolis and Others* [1992] 2 WLR 50). Any objections should be considered and advance notice should be provided of an intention to disclose regardless. Notice does not have to be given when it would be inappropriate or impracticable to provide notice, for example if it would prejudice an investigation by the law enforcement agency requesting the information (*R (on the application of Kent Pharmaceuticals Ltd) v. Serious Fraud Office and another* [2004] All ER (D) 191 (Nov)).

Section 3 of the Criminal Justice Act 1987 further limits disclosure by the SFO to third parties. Information obtained during the course of an investigation by the SFO can only be disclosed to certain specific government departments or bodies, or competent authorities specified in the Act, and only for the purposes of any criminal investigation or criminal proceedings, whether in the UK or abroad and for the purposes of assisting any public or other authority under the order. The list of competent authorities is wide and includes anybody having supervisory, regulatory or disciplinary functions; however, it does not include liquidators, provisional liquidators, administrators or administrative receivers.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

In these circumstances, the company should not provide the documents, but should inform the requesting authority of the reason why these documents cannot be provided (i.e., that the data protection laws in the other country constitute reasonable excuse for lack of compliance).

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

The collection and use of personal data in the UK are governed by the DPA 2018, including restrictions on the disclosure of personal data. Personal data is defined as data that relates to a living individual who can be identified from that data. However, broadly speaking, the non-disclosure provisions in the DPA 2018 do not apply if the material is requested by a notice or court order issued on the grounds that the material is necessary for the prevention or detection of crime, the apprehension or prosecution of offenders, the assessment or collection of any tax or duty, or of any imposition of a similar nature.

The term 'blocking statute' is generally not applicable except in the field of financial and trade sanctions, for which there is blocking legislation in relation to specific US sections that have extraterritorial application.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

When material is provided voluntarily and without restrictions, the authority is free to share it with third parties or other authorities, and to use it for any purpose.

In general, it is advisable only to provide material voluntarily having obtained contractual undertakings that agree the restricted basis on which the material has been provided (e.g., only for use by that authority in the course of an investigation and not to be shared with other parties).

While contractual undertakings restrict an authority's ability to voluntarily provide material to other parties, they do not prevent third parties from obtaining court orders against the authority requiring production of the material. However, production orders should only be granted when it is in the interests of justice, and the fact that the material came into the possession of the authority under the restrictions imposed by the undertakings may lead a court to determine that it is not appropriate to grant a production order against the authority in that context, particularly as the third party could attempt to obtain the documents from an unfettered source, such as the company.

In general, authorities are restricted as to how they can share material they obtain as a result of exercising their compulsory powers or court orders, and customarily such material should only be shared where it is necessary for an investigation and the disclosure is proportionate.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Penalties on conviction include imprisonment for individuals, fines, compensation and confiscation orders. Individuals can also be disqualified from being a director of a company for up to 15 years. When DPAs are agreed, monitoring may be imposed.

Companies convicted of certain offences, including active bribery and money laundering, must also be debarred from public tendering for up to five years.

Regulatory authorities can impose additional penalties. For example, the FCA can withdraw a firm's authorisation and prohibit it from undertaking specific regulated activities for up to 12 months, prohibit individuals from carrying out regulated activities, or impose fines on firms or individuals. The Prudential Regulation Authority (the authority responsible for the prudential regulation and supervision of around 1,700 banks and other firms) can restrict a firm's permission to conduct regulated activities or impose a fine.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

The Public Sector Procurement Directive (2014/24/EU) was transposed into UK law by the Public Contracts Regulations 2015. Under these Regulations, companies must be excluded from public procurement if they have been convicted in the past five years of any offences from a list that includes, among others, conspiracy, corruption, bribery, money laundering and fraud. The corporate offence of failure to prevent bribery (section 7 of the Bribery Act 2010) is not included in this list of offences and does not require mandatory debarment.

The Regulations also provide a list of offences that carry discretionary debarment for up to three years, including professional misconduct, non-payment of tax and distortion of competition.

However, the Regulations allow companies to recover eligibility to bid for public contracts following a debarment by demonstrating evidence of self-cleaning, such as the payment of compensation to the victim of the offending, clarification of the facts and circumstances of the offence in a comprehensive manner, co-operation with the investigating authority, and the implementation of appropriate measures to prevent further criminal offences or misconduct.

64 What do the authorities in your country take into account when fixing penalties?

When fixing penalties following conviction, courts must have regard to the sentencing guidelines published by the Sentencing Councils for England and Wales, and Scotland.

Specific sentencing guidelines were published in 2014 for England and Wales in respect of corporate fraud, bribery and money laundering offences providing that, when sentencing a company, the court must first determine whether compensation or confiscation orders should be made.

Thereafter, the court should consider, inter alia, the following issues:

- the level of culpability and financial harm;
- the aggravating or mitigating factors, for example whether the criminal activity was endemic or whether the corporate offered full co-operation with the law enforcement authority during the investigation;
- the financial circumstances of the company; and
- the stage at which a guilty plea was entered (if the matter was not contested).

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

DPAs have been available in England and Wales (as a result of the Crime and Courts Act 2013) since 2014 as an alternative disposal for corporate offending. DPAs are not currently available in Scotland, where a civil settlement regime applies, or in Northern Ireland. Non-prosecution agreements do not exist in the UK.

The SFO and CPS have published a Code of Practice explaining the DPA process. Also, in summer 2019, the SFO issued guidance on what it considers amounts to co-operation with its investigations, including a requirement to report a suspected fraud or bribery within a reasonable time of the suspicion arising. The guidance makes it clear that co-operation will be a relevant factor in making charging decisions.

A prosecutor may invite, at its discretion, a corporate suspect into DPA negotiations if it determines that having identified the full extent of the offending, the evidential test has been satisfied and the public interest would benefit from a DPA. Until the *Rolls-Royce* case, the orthodox view was that a corporate will only be invited to negotiations where a self-report has been made and the corporate has fully co-operated with the authority. Following *Rolls-Royce*, it is possible that a DPA may be negotiated in wider circumstances, including when there has been no self-report but subsequent extraordinary co-operation by a corporate with the law enforcement authority.

If it is possible to agree the terms of a DPA and a statement of facts, the corporate will be formally charged with the criminal offence or offences and the matter will be brought before a judge for approval. The judge will only approve the DPA if satisfied that it is in the interests of justice and the terms are fair, reasonable and proportionate. The judge can adjourn the matter to obtain further information or clarification as to the facts or terms.

If judicial approval is given, the criminal proceedings will be suspended for a set period as defined by the terms of the DPA. The terms and facts of the DPA will then be published on the authority's website.

If the corporate complies with the terms of the DPA, at the conclusion of the set period the criminal proceedings will be formally discontinued. If the corporate breaches the terms and the breach cannot be remedied, the criminal proceedings will resume.

DPAs carry the advantage of avoiding a conviction, affording the opportunity of speedier resolution (relatively speaking) and to continue trading under agreed parameters. They also enable the corporate to avoid the time and costs of an open-ended, lengthy and uncertain criminal investigation and trial that can adversely affect share price and access to finance, and cause difficulties in tendering.

The obvious disadvantage of entering into a DPA is if a corporate has substantially accepted its conduct would have constituted a criminal offence, and then will need to accept penalties based on a prosecution case that has not been tested at trial, where a corporate could potentially have been acquitted of the relevant charges (as in the *Tesco Stores Limited* case, as discussed in question 51). A further disadvantage to be carefully considered is that the terms of a DPA are likely to include regular monitoring and audit by an independent monitor (typically a large accountancy or law firm) for which the company will bear the costs.

At the time of writing, five DPAs have been agreed in the UK. The most recent of these was with Serco Geografix Ltd (a wholly owned subsidiary of Serco Group plc), relating to allegations of fraud and false accounting. Of particular significance was the 'very substantial co-operation' shown by Serco Group, which included not only waiving privilege in respect of certain accounting material and detailed, proactive and prompt reporting of the fraudulent conduct, but also co-operation with the SFO's request not to engage in any internal inquiry of its own by way of interviewing witnesses during the SFO's criminal investigation; instead Serco Group instructed an independent law firm to conduct a full document review and provided the SFO with a detailed report of the findings. It also notified the SFO of any developments within the business that could affect the criminal investigation and gave the SFO unrestricted access to the email accounts of current and former employees. This is also the first case in which a parent company agreed to accept obligations mirroring the requirements imposed on its subsidiary by the DPA, described by Mr Justice Davis as a 'key component of the DPA' and 'an important development in the use of DPAs'.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Reporting restrictions can be placed on DPAs while criminal proceedings in relation to connected individuals are under way in the UK. Reporting restrictions were imposed on the Sarclad and Tesco DPAs because of ongoing proceedings against the individuals allegedly responsible for the misconduct. Following the conclusion of those proceedings, the reporting restrictions were lifted.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Before entering into a settlement with a law enforcement authority, a company should assess: the merits and strength of the prosecution and defence cases; the likelihood of conviction; the expected time, cost, reputational damage and other adverse effects of a lengthy investigation and trial; and the likely penalties in the event of a conviction, including possible debarment from public procurement tenders.

The company should then carefully assess the terms of the proposed settlement, including the effect that continuing co-operation could have on the business (legal costs, staff resources, etc.); whether the settlement will resolve the matter in all relevant jurisdictions and, if not, the effect the settlement could have in regard to ongoing investigations in other jurisdictions (e.g., whether the authority that has settled will disclose information and assist foreign authorities); and any other adverse effects that the settlement could have on the future of the business.

Ultimately the company should balance the seriousness of the charge and the potential consequences of a conviction (including whether it results in debarment) against the terms of the settlement, as in some circumstances the terms of a settlement, including, for example, the costs of regular review and monitoring by an independent monitor (typically a large accountancy or law firm), could be more disadvantageous to a company than a conviction.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

The Crime and Courts Act 2013 and the related guidance permit the appointment of monitors in appropriate cases. The Deferred Prosecution Agreements Code of Practice (the DPA Code) – of which the SFO and CPS are required to take account when negotiating, applying to the court for and overseeing DPAs – sets out the roles, duties and mechanics of appointing monitors as a term of a DPA. The DPA Code stops short of requiring or even encouraging the appointment of a monitor as a condition of a DPA.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Parallel private civil actions are allowed. Generally, but not always, the criminal proceedings will take precedence and civil proceedings can be stayed for the duration of the criminal investigation, so as not to prejudice any criminal proceedings.

Private plaintiffs will only gain access to specified information in the authority's files if they obtain a court order. Before making any such order, the court would carefully consider the reason why the private plaintiff requires the information, whether the plaintiff would be able to obtain the information from any other source, the method by which the authority obtained the relevant information, for example if it was obtained under compulsory powers, and whether the information is likely to contain any confidential, privileged or personal information relating to third parties.

Increasingly, small numbers of private criminal prosecutions involving allegations of fraud are being conducted in the courts of England and Wales. The instigation of a private prosecution is provided for in section 6 of the Prosecution of Offences Act 1985 and is subject to a power of the director of public prosecutions to take over the private prosecution at any stage (and, if they choose, to discontinue it).

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

It is a contempt of court to publish a report that creates a substantial risk that the course of justice in active criminal proceedings will be seriously impeded or prejudiced. Proceedings are active for this purpose after arrest or charge and until the proceedings have been concluded, for example by acquittal or conviction, or discontinuance by the authority. As a result there is generally very little media reporting of criminal investigations in the UK until the end of a trial other than to state the facts of arrests and report court hearings.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is common practice for companies to hire a public relations (PR) firm to manage a large-scale corporate crisis to mitigate potential reputational damage. It is important to ensure

a consistent approach by opening good lines of communication between the company's internal marketing and the external PR firm, and to ensure that the PR firm is aware of any legal or corporate issues (including any agreements reached with the investigating authority with regard to press releases, etc.).

It is also vitally important that public statements do not have the potential effect of prejudicing ongoing criminal proceedings (for example, the trial of the company or individual employees) or contradict any defence on which the company may later seek to rely. For those reasons, statements issued by a company under investigation should be brief and factual, and should always be approved by the company's criminal law advisers.

72 How is publicity managed when there are ongoing related proceedings?

As stated in question 71, it is vitally important that public statements issued by the company do not have the potential effect of prejudicing ongoing criminal proceedings, such as the related prosecution of employees or third parties. Statements issued by a company in those circumstances should always be brief and factual, and approved by the company's criminal law advisers until the conclusion of all related proceedings.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Under the UK Listing Rules, publicly listed companies must issue a market announcement without delay regarding any major new development that may affect their business, if the development may lead to a substantial share price movement. A settlement of criminal proceedings would generally require such an announcement.

If the matter is settled by way of a DPA, the matter is not settled until it has actually been approved by a judge at a court hearing. In practice, prior to the final hearing (at which the parties will generally expect approval to be given, as the terms, etc. will have been examined and challenged at preliminary hearings), the company and the authority will have agreed press statements to be released to the market and wider public as soon as approval is given.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

The UK government is due to report on its call for evidence in expanding the 'failure to prevent' offence to include other economic crime (it currently covers bribery and tax evasion).

In April 2018, the European Parliament voted to adopt the Fifth Money Laundering Directive (5MLD). Intended to address weaknesses and update 4MLD, it is to be transposed into UK domestic law by 10 January 2020; however, it is presently unclear whether the UK government will proceed with the legislation in the event of a no-deal Brexit.

5MLD makes significant changes to the anti-money laundering regime in the European Union, including designating virtual currency platforms and custodian wallet providers as obliged entities for the purposes of 4MLD and revising the scope of the customer due

diligence provisions. It will also require enhanced due diligence to be carried out in transactions to and from high-risk countries; increase powers and access to information for national financial intelligence units; and require registers of corporates' beneficial ownership information to be made available to the general public.

In June 2019, the Law Commission published its report on the suspicious activity reporting process, concluding that although the core of the current system should be retained, improvements and efficiencies are required if the reporting regime is to produce useful intelligence rather than simply volumes of low-quality information. Recommendations include:

- the creation of an advisory board of industry experts to oversee the drafting of guidance and advise the secretary of state on appropriate improvements and how best to respond to emerging threats;
- the production of a new standardised online suspicious activity report (SAR) form, to make the reporting process easier to navigate, promoting greater consistency in the information that is provided in an easy-to-read, accessible format that would also allow analytical techniques to be applied to it, and speed up the process; and
- allowing ring-fencing of suspected criminal property by a credit of financial institution in certain circumstances. The practical effect of submitting an SAR is that whole accounts are frozen, not just the allegedly criminal property element, which can cause difficulties for both banks and account holders while a decision on consent to proceed is awaited (and even after that). This recommendation will give some comfort particularly to banks, allowing for a more proportionate response to the reporting of suspected criminal property, enabling transactions on legitimate funds to continue while prohibiting the use of those under suspicion.

The UK government's response to the recommendations is awaited.

29

United States

Jennifer L Achilles, Francisca M Mok, Eric H Sussman and Bradley J Bolerjack[1]

General context, key principles and hot topics

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

According to published reports, a significant criminal investigation is being conducted in connection with the computer issues that contributed to two crashes involving the 737 Max (in October 2018 and March 2019). This could, as a minimum, result in civil actions or criminal charges (or both) being pursued against corporations involved in the aviation industry or executives at some of those companies, depending on the facts that emerge from that investigation.

Numerous cases have been filed against drug manufacturers and distributors in connection with the distribution of opioids in the United States. While these are predominately civil cases, in some instances prosecutors are evaluating criminal charges against involved individuals.

2 Outline the legal framework for corporate liability in your country.

Under the doctrine of *respondeat superior*, a corporation may be held criminally liable for the illegal acts of its directors, officers, employees and agents. The government must establish that the corporate agent's actions were (1) within the scope of his or her duties and (2) intended, at least in part, to benefit the corporation. The corporation need not have profited from the agent's actions for the corporation to be held liable. Prosecutors in the United States are given broad discretion to determine whether to prosecute for violations of federal criminal law.

1 Jennifer L Achilles, Eric H Sussman and Bradley J Bolerjack are partners and Francisca M Mok is the Century City managing partner at Reed Smith LLP.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Corporations are subject to regulation and oversight by federal, state and local authorities depending on their businesses and industry. It is not uncommon for multiple government authorities to conduct investigations at the same time regarding the same set of facts, and agencies do not typically refrain from pursuing cases because other agencies are also involved. The Department of Justice (DOJ) has policies and protocols relating to corporate prosecutions, as well as a policy to work with other agencies investigating the same conduct to avoid 'piling on' penalties.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

There is no threshold of suspicion that must be met before law enforcement may initiate an investigation. Investigations may even be initiated and conducted to satisfy law enforcement that no misconduct occurred.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

Civil subpoenas issued by government agencies can be challenged in court with respect to the lawfulness or scope of a subpoena. However, typically, the relevant government agency has broad authority to obtain information that is relevant to a legitimate subject of investigation.

6 Does your country make use of co-operative agreements giving immunity or leniency to individuals who assist or co-operate with authorities?

Both individuals and corporations can benefit from co-operating with law enforcement during an investigation. Individuals may enter into agreements with the government by which they will be granted immunity or be permitted to plead guilty to a lesser charge in exchange for agreeing to provide information or testimony against other defendants. Corporations may receive non-prosecution agreements (NPAs) or deferred prosecution agreements (DPAs) in exchange for co-operating in an investigation.

7 What are the top priorities for your country's law enforcement authorities?

Some top law enforcement priorities affecting corporations include enforcement of the False Claims Act (prohibiting overcharging and related false claims for payment by the government); securities laws regulating publicly traded companies and the stock market; anti-bribery and anti-corruption laws; cybersecurity; and laws governing consumer online privacy.

Cyber-related issues

8 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

The United States does not have an overarching federal cybersecurity law; rather, certain government agencies and banking regulators have created cybersecurity regulations for the corporations under their control.

For example, issuers of US securities are required to comply with the Securities and Exchange Commission's (SEC) regulations, including: (1) Regulation S-P (17 CFR section 248.30), which requires firms to adopt written policies and procedures to protect customer information against cyberattacks and other forms of unauthorised access; (2) Regulation S-ID (17 CFR section 248.201-202), which outlines a firm's duties regarding the detection, prevention and mitigation of identity theft; and (3) the Securities Exchange Act of 1934 (17 CFR section 240.17a-4(f)), which requires firms to preserve electronically stored records in a non-rewritable, non-erasable format. Since 2015, the SEC has brought a handful of enforcement actions against public companies for violations of these regulations.

All 50 US states have state-specific cybersecurity laws. The states require companies to inform consumers if their personal information was compromised or may have been compromised. In many cases, state attorneys generally work together to bring coordinated, multi-state data breach actions. For example, when Marriott announced that there had been a breach of its reservation systems, exposing the personal data of up to 500 million customers, multiple states announced the opening of investigations.

State banking regulators also have cybersecurity requirements and often coordinate enforcement efforts. The New York Department of Financial Services and seven other state banking regulators announced that Equifax had agreed to take corrective action for its 2017 data breach.

9 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

Most cybercrime is prosecuted under the US Computer Fraud and Abuse Act (CFAA). The CFAA criminalises the unauthorised access of a protected computer without proper authorisation. It covers hacking, phishing, infection of IT systems with malware, electronic theft, and identity theft or fraud. Additional US statutes that cover cybercrime are 18 USC section 1028, which criminalises identity theft; 18 USC section 1029, which criminalises the use of unauthorised access devices to commit fraud; and the Stored Communication Act (18 USC section 2701), which criminalises electronic theft of stored communications. The DOJ has a Computer Crime and Intellectual Property Section that investigates and prosecutes computer crimes.

The US and 60 other jurisdictions have signed the Budapest Convention on Cybercrime, which is a binding international treaty that provides a framework for international co-operation on cybercrime and electronic evidence.

Cross-border issues and foreign authorities

10 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

In *RJR Nabisco, Inc. v. European Community* (2016), the US Supreme Court set up a two-step framework for addressing the extraterritorial application of federal statutes. First, a court must determine whether the presumption against extraterritoriality has been rebutted through a clear, affirmative indication that the statute applies extraterritorially. If not, the court must determine whether the case involves a domestic application of the statute. If the relevant conduct occurred within the United States, even if some conduct occurred abroad, the case is deemed an acceptable domestic application of the statute. On the other hand, if the conduct that is the statute's focus occurred abroad, extraterritorial application is not permitted.

The Foreign Corrupt Practices Act is an example of a statute that states that it can be applied against foreign companies or persons who carry out bribery schemes while acting in the United States. Since 2010, the US courts have narrowly construed the extraterritorial reach of a number of other statutes, including the Alien Tort Statute, the Torture Victim Protection Act and the Securities and Exchange Act of 1934.

11 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

The combination of data protection regimes, blocking statutes, bank secrecy laws and employment laws outside the United States make cross-border investigations challenging. The DOJ has broad discretion to provide co-operation credit and leniency to corporations that turn over relevant facts in a timely manner. Corporations that have relevant documents outside the United States must weigh the risk of violating foreign laws against the risk that the US government will bring criminal charges against it.

12 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

Double jeopardy does not prevent the US government from charging a corporation with a crime even if the corporation has already resolved similar charges with a foreign government. According to the dual-sovereignty doctrine, a crime under one sovereign's laws is not 'the same offence' for double jeopardy purposes as a crime under the laws of another sovereign.

In May 2018, the DOJ adopted a non-binding policy into the Justice Manual that promotes coordination between US and foreign law enforcement in an effort to limit duplicative penalties on corporate entities for the same conduct. The policy instructs prosecutors that in resolving a case with a company that is being investigated by multiple authorities, the DOJ and others should coordinate with one another to avoid the unnecessary imposition of duplicative penalties against the company.

13 Are 'global' settlements common in your country? What are the practical considerations?

Global resolutions are becoming more common as US law enforcement increases its co-operation with law enforcement in other countries. Global settlements can benefit a corporation by presenting an efficient way to resolve issues with multiple countries at once. However, global settlements do not always result in overall reduced penalties and fines, as law enforcement authorities may make higher settlement demands than they would have made individually. Corporations should proceed cautiously when negotiating global settlements and be sure to invoke any applicable policies against 'piling on'.

14 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

A criminal decision against a corporation in another jurisdiction will not end an ongoing investigation in the United States. US law enforcement may attempt to co-operate with foreign authorities to gain additional facts about the corporation that it has been unable to get directly. US law enforcement may also consider the penalties and fines imposed by the foreign authority when deciding an appropriate penalty in the United States.

Economic sanctions enforcement

15 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury enforces economic and trade sanctions against targeted foreign countries and individuals, and takes action against those who do business with them. Primary sanctions prohibit transactions with sanctioned countries or persons. Primary sanctions apply to US persons, US corporations and all persons physically located in the United States, regardless of nationality. Non-US entities can also be liable for primary sanctions for taking actions within the United States, conspiring with US persons to violate sanctions, or using the US financial system. Secondary sanctions may be imposed on non-US persons or entities who engage in transactions deemed to be contrary to US national security and foreign policy interests. Although penalties cannot be imposed for secondary sanctions, they can result in restricting access to the US financial system or markets. OFAC has brought several high-profile cases against non-US financial institutions in recent years.

16 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

OFAC enforcement actions have increased significantly as compared with prior years. In the 12 months ending 30 June 2019, OFAC reported bringing 25 published enforcement actions as compared with nine the previous year. The level of penalties has increased as well, from US$17.1 million for the year ending 30 June 2018 to approximately US$1.35 billion the following year.

OFAC recently announced a change in policy that may end up increasing a corporation's overall penalty in cases involving multiple US agencies. In June 2019, OFAC stated that the only penalties charged by another agency that OFAC would deem to satisfy its own penalties would be those that fit the same pattern of conduct over the same period of time that gave rise to the OFAC penalty.

17 Do the authorities responsible for sanctions compliance and enforcement in your country co-operate with their counterparts in other countries for the purposes of enforcement?

The US Treasury Department and OFAC co-operate with their counterparts in countries that are allies of the United States.

18 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

The US has not enacted blocking legislation.

19 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

Not applicable.

Before an internal investigation

20 How do allegations of misconduct most often come to light in companies in your country?

Common ways in which misconduct comes to light include regular audit and compliance activities, whistleblower complaints, government subpoenas, media reports, and business people encountering irregularities in the ordinary course of their jobs.

Under the federal securities laws, when auditors become aware that an illegal act may have occurred at a public company, certain affirmative investigation and reporting obligations are triggered. The auditor is obliged to determine whether an illegal act has occurred, report it to management and assure itself that the issuer's audit committee or board of directors has also been informed. There are additional reporting obligations imposed on the auditor if the issue is not remedied, which culminate with auditor withdrawal and affirmative reporting to the SEC of the issue.

Information gathering

21 Does your country have a data protection regime?

The United States does not have a data protection regime.

22 To the extent not dealt with above at question 8, how is the data protection regime enforced?

Not applicable.

23 Are there any data protection issues that cause particular concern in internal investigations in your country?

Not applicable.

24 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

There is no general restriction on interception of employee communications in the United States so long as the employees are using company systems.

Dawn raids and search warrants

25 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Ordinarily, US law enforcement uses subpoenas for information to obtain materials from companies. It is unusual for law enforcement to conduct a dawn raid or execute a search warrant at a company. The use of these tools generally indicates a concern that the company may either conceal or destroy relevant evidence if it was requested by a subpoena.

A search warrant allows law enforcement to search for materials specifically delineated in the warrant. While a search warrant requires a company to provide access to these materials, it does not require employees of the company to submit to interviews or answer questions posed by law enforcement. If law enforcement exceeds the limits of a search warrant or conducts improper interviews, the company's primary recourse would be to move to suppress the information in any subsequent legal proceeding.

26 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

Law enforcement agencies bear the responsibility for segregating privileged materials or using a special 'taint team' of attorneys unrelated to the investigation to review seized documents for privilege. Ordinarily, companies will not be permitted to withhold privileged documents without consent of law enforcement. Companies can assist in the privilege review process by identifying in-house and external attorneys to the investigative agents. Companies can also be careful to segregate these materials to protect against inadvertent disclosure.

27 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

Under the Fifth Amendment to the US Constitution, an individual cannot be compelled to provide incriminating testimony against himself or herself. Any testimony improperly compelled cannot be used in a legal proceeding against the individual. Companies, however, are not protected by this privilege and cannot withhold testimony that might be incriminating.

Generally, there is no right against self-incrimination for producing documents, unless the act of producing the documents would be incriminating.

Whistleblowing and employee rights

28 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The United States does not have a comprehensive framework for protecting all whistleblowers in all situations. Instead, many different federal and state laws have been enacted to incentivise whistleblowers and protect them from retaliation. For example, the False Claims Act allows persons and entities with evidence of fraud against federal programmes or contracts to sue the wrongdoer on behalf of the government. A *qui tam* plaintiff can receive between 15 and 30 per cent of the total recovery from the defendant.

Additionally, the whistleblower programme under the Dodd-Frank Act provides monetary incentives for individuals to report possible violations of the federal securities laws to the SEC. Under the programme, eligible whistleblowers are entitled to an award of between 10 and 30 per cent of the monetary sanctions collected. The whistleblower programme also prohibits retaliation by employers against employees who provide the SEC with information.

29 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Aside from any applicable whistleblower protections, employees generally do not have rights under federal or state employment laws during an investigation. This is true whether the employee is an officer, director or rank-and-file employee.

30 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

Unless whistleblower protections apply, a company may take any number of disciplinary actions against an employee who has engaged in misconduct, including suspension or termination of contract. Companies have a duty to their shareholders to take action and not turn a blind eye to misconduct.

31 Can an employee be dismissed for refusing to participate in an internal investigation?

Most employees in the United States are subject to at-will employment, meaning that, unless other protections apply, their contracts may be terminated at any time. Employees whose conduct is within the scope of an investigation are expected to participate in investigations, and may be dismissed if they refuse to co-operate.

Commencing an internal investigation

32 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

It is common to have a working investigative plan to manage investigative activities. Such a document may address:

- document preservation and gathering;
- witnesses;
- legal issues and analysis;
- factual analysis;
- key questions to be answered; and
- reporting obligations.

However, because investigations are often fluid, the expectation is that the document will be updated and revised frequently, to account for new or different tasks based on information learned in the course of the investigation.

33 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

A company should conduct an internal investigation and remediate the issue. Most government agencies give corporations credit for investigating and self-reporting issues. The decision to self-report is fact dependent and involves weighing many factors.

Under the SEC's regulations, an in-house lawyer at a public company is required to report 'evidence of a material violation' to the issuer's chief legal officer and chief executive officer, and in some cases to the appropriate committee of the issuer's board of directors consisting solely of independent directors, or to the whole board of directors. In the context of an investigation initiated by a public company's external auditors, the company may have an obligation to report to the SEC if the auditors conclude that the company has not properly remediated certain illegal activities.

34 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

The company should prepare a legal hold notice and distribute it to relevant individuals and the company's IT department. Affirmative steps should be taken to prevent destruction of responsive materials – including discontinuing any automatic deletion of such data pursuant to data retention policies.

If the company is being investigated for potential wrongdoing, it is important that external counsel or individuals with indicia of independence and trustworthiness are responsible for preserving and collecting documents. If there is any uncertainty regarding what search terms should be used to identify responsive documents, attorneys for the corporation typically discuss search terms with the government.

35 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

As a general matter, there is no requirement to disclose the existence of an internal investigation or the fact that the company was contacted by law enforcement. Public companies are forbidden from making affirmative statements that are false or misleading. Thus, companies should be careful not to make statements that are untrue or misleading because of undisclosed facts about an internal investigation or law enforcement contact. There is a duty to disclose to the extent that disclosure is necessary to ensure affirmative statements are not misleading.

36 How are internal investigations viewed by local enforcement bodies in your country?

Government authorities place value on independent and thorough internal investigations. For example, the DOJ in its Justice Manual has stated that to 'earn maximum co-operation credit, a corporation must do a timely self-analysis and be proactive in voluntarily disclosing wrongdoing and identifying all individuals substantially involved [ ] or responsible' (Justice Manual, section 4-3.100(3)). The SEC describes self-reporting as one of the key factors for evaluating a company's co-operation 'including conducting a thorough review of the nature, extent, origins and consequences of the misconduct, and promptly, completely and effectively disclosing the misconduct to the public, to regulatory agencies, and to self-regulatory organizations' (SEC Enforcement Manual, Framework for Evaluating Co-operation by Companies, 6.1.2). Neither agency sets forth exacting requirements for the conduct or format of the internal investigations; what is appropriate is fact-dependent.

Attorney–client privilege

37 Can attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Generally, the attorney–client privilege and the attorney work-product doctrine may be claimed over most aspects of an internal investigation so long as the fact-finding and analysis is being done by or at the direction of attorneys for the purpose of providing legal advice to the client. This privilege would cover attorney notes, interview memoranda, legal analysis and recommendations provided by counsel to the client. Companies should ensure that privileged materials are not shared with third parties and are clearly labelled as being 'attorney–client privileged'.

38 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

Communications by corporate employees made for the purpose of assisting counsel in providing legal advice to the corporation are generally covered by attorney–client privilege. The corporation holds the privilege and it may only be waived by the corporate entity or an authorised executive (for example, the general counsel).

39 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

The attorney–client privilege applies equally to in-house and external counsel so long as both are providing legal advice. In certain instances, in-house counsel will be called on to provide 'business' advice, which is not protected even if it is provided by an attorney.

40 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to (internal or external) investigations in your country?

The attorney–client privilege applies equally to US and foreign lawyers.

41 To what extent is waiver of the attorney–client privilege regarded as a co-operative step in your country? Are there any contexts where privilege waiver is mandatory or required?

While the waiver of the attorney–client privilege is regarded as a co-operative step by US law enforcement, DOJ policy prohibits law enforcement from requesting or requiring privilege waivers to receive credit for co-operation. Other federal agencies may request but do not typically require privilege waivers to obtain co-operation credit.

42 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Most courts will not enforce 'selective waivers' to government entities. Companies sometimes provide factual information to the government (rather than any legal analysis or memos) to avoid an argument by a third party that privilege has been waived.

43 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

If the disclosure of attorney–client information was compelled in a foreign country (or the privilege was not recognised), this would generally not result in a waiver of the attorney–client privilege in the United States. However, any voluntary disclosure will usually result in a waiver.

44 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege does exist in the United States. It is an extension of the attorney–client privilege to communications between two or more parties that have a common legal interest. The party asserting the privilege must demonstrate that (1) the communications were made in furtherance of a joint defence effort, (2) the statements were designed to further that effort and (3) the privilege was not waived.

45 Can privilege be claimed over the assistance given by third parties to lawyers?

So long as a third party is working for a client at the direction of an attorney, and for the purpose of assisting the lawyer to provide legal advice to the client, this assistance will remain privileged.

Witness interviews

46 Does your country permit the interviewing of witnesses as part of an internal investigation?

Yes, witness interviews are a critical part of internal investigations in the United States.

47 Can a company claim attorney–client privilege over internal witness interviews or attorney reports?

Yes, companies regularly assert privilege over witness interviews and reports in the United States, provided that the interviews and reports were generated to provide legal advice.

48 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

Upjohn warnings are required when conducting witness interviews of employees and are typically provided to both current and former employees.

49 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

Witness interviews are typically conducted by external counsel, sometimes in the presence of in-house counsel or subject matter experts assisting counsel (or both). Documents are usually shown to the witness during interviews. Witnesses can retain their own legal representation if they so choose, but there is no requirement to do so.

Reporting to the authorities

50 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

There is no overarching duty or legal obligation to self-report corporate misconduct, but there are certain specific situations in which it is mandatory, including highly regulated industries such as insurance, banking and healthcare.

51 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

The DOJ and several other federal agencies have issued policies providing for leniency and reduced penalties for companies that self-report. It is generally understood that co-operating with a government investigation will not result in as favourable an outcome for a corporation as the combination of self-reporting and co-operating. In some cases, self-reporting corporate misconduct and co-operating with an investigation can lead to a decision not to prosecute.

Despite the strong incentive to self-report, it is not always the best course of action. Several factors must be considered, such as the severity and pervasiveness of the misconduct;

whether corporate officers or board members were involved; whether the misconduct continued over a long period of time; and whether the investing public or consumers were harmed by the misconduct.

52 What are the practical steps you need to take to self-report to law enforcement in your country?

There is no formal process for self-reporting. Typically, external counsel will contact law enforcement and seek a meeting to explain how the misconduct was discovered, how the misconduct occurred, and what the corporation is doing to investigate and make sure the misconduct is not repeated. One of the factors the government considers is whether the company reported within a reasonable time after learning of the misconduct. Accordingly, a complete internal investigation is not required prior to self-reporting, although the company will want to understand enough facts to determine whether self-reporting is advisable.

Responding to the authorities

53 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

The first step following receipt of a subpoena would ordinarily be for external counsel to place a call to the government attorney. The purpose of the call would be to understand the nature and scope of the government's investigation, as well as whether the company is a target of the investigation or simply a witness. Most law enforcement agencies will enter into a dialogue with a company's external attorney prior to charges being brought. Most prosecutors' offices will also allow a company's attorney to meet with senior supervisors in the prosecutors' office to present their position as to why charges should not be brought.

54 Are ongoing authority investigations subject to challenge before the courts?

Investigations are considered to be firmly within the discretion of the executive branch of government. Unless there is evidence that government prosecutors are abusing their investigative authority and violating legally protected rights, it is highly unusual for courts to interfere with an ongoing investigation.

55 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

When a company receives multiple subpoenas regarding the same facts, the company should analyse whether this is part of a coordinated effort or whether these are entirely separate investigations. If they are coordinated investigations, it can be advantageous to ensure consistent disclosure between all jurisdictions. If they are separate investigations, it may not be advantageous to alert US authorities that foreign authorities are investigating the same issues.

56 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for, and produce material, in other countries to satisfy the request? What are the difficulties in that regard?

Prosecutors typically expect a company to search for and produce responsive documents in its possession, custody or control even if those documents are located outside the United States. Documents held by a company's foreign affiliates are generally considered in the company's control. If the subpoenaed documents implicate the laws of another jurisdiction, such as data privacy laws, the company should consider whether there is a way to comply with the law while also complying with the subpoena (such as by requesting the consent of employees whose data will be turned over). If responding to the subpoena would expose the company and its employees to criminal liability in another country, the company may decide to seek a protective order from a US court.

57 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for co-operation with foreign authorities?

It is common for US law enforcement to share investigative materials with authorities outside the United States, particularly when the information sharing is mutual. Sometimes co-operation occurs through formal mutual legal assistance treaties or memoranda of understanding.

58 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Unless law enforcement agrees to be bound by a non-disclosure agreement, the government can share materials received during an investigation with other agencies or overseas investigators. The government does not typically share information with non-government third parties or allow the material to be subject to public disclosure during the course of an investigation. There are strict secrecy laws for information obtained in the United States via a grand jury subpoena. This information cannot be shared without a court order, or else under very narrow legal exceptions.

59 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

A company should not voluntarily produce documents to US law enforcement if doing so would violate the laws of another country. If the company is compelled to produce them by subpoena, the least risky solution is to obtain consent from the foreign country or ask law enforcement to obtain the documents through a mutual legal assistance treaty. If those options fail, the company could seek a protective order in court, seeking to be relieved of its obligation to produce such documents. If the court denies the company's motion for a protective order, the company will have to decide whether it is more risky to continue to resist the subpoena or to comply and violate foreign law.

60 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Not applicable.

61 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

In some cases, there are no additional risks in producing documents voluntarily versus pursuant to a subpoena. In other cases, however, such as when the government requests otherwise confidential information about customers or third parties, it is less risky to produce documents pursuant to subpoena. Voluntary production may subject a company to potential liability from third parties for providing confidential information to law enforcement that was not compelled.

Documents produced to the government during the course of an investigation are exempt from public disclosure under the Freedom of Information Act during the pendency of the investigation. Information compelled by a grand jury subpoena is ordinarily protected by strict secrecy and would not be discoverable by third parties, whereas similar information that was voluntarily provided would be discoverable.

Prosecution and penalties

62 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

If a company is convicted of a crime, it can be sentenced to fines, restitution, disgorgement, forfeiture of property derived from criminal activity, and suspension or debarment. Corporate monitors are also sometimes appointed to oversee a company's ongoing activities. Individuals are subject to similar criminal penalties in addition to imprisonment.

63 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

Depending upon the context of the investigation, suspension or debarment is a significant risk in heavily regulated industries, such as healthcare and securities. When negotiating with regulators, counsel may be able to negotiate terms that would avoid or minimise the risk of these possibilities and the attendant impact on future business operations. Extraterritorial settlements are not typical because such arrangements tend not to resolve violations of US law.

64 What do the authorities in your country take into account when fixing penalties?

In the event of a successful conviction, sentencing courts consider factors set forth in the US Sentencing Guidelines as well as criminal statutes and policy guidelines. In general,

the broad factors to be considered at sentencing are set forth at 18 USC section 3553(a) and include:

- the nature and circumstances of the offence and the history and characteristics of the defendant;
- the need for the sentence imposed to reflect the seriousness of the offence, promote respect for the law and provide just punishment for the offence;
- to afford an adequate deterrent to criminal conduct;
- to protect the public from further crimes of the defendant;
- to provide the defendant with the necessary educational or vocational training, medical care or other correctional treatment in the most effective manner;
- the kinds of sentences available;
- the kinds of sentence and the sentencing range established for the applicable category of offence committed by the applicable category of defendant as set forth in the US Sentencing Guidelines or applicable policies; and
- the need to provide restitution to any victims of the offence.

Resolution and settlements short of trial

65 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Both are available in the United States.

Under the terms of an NPA, the government agrees not to file a criminal charge for the specified acts under investigation. In exchange, the putative corporate or individual defendant enters into certain agreements with the government, which may include financial terms, imposition of a corporate monitor or other remedial actions. The advantage of such an agreement from the defendant's perspective is that no criminal charge is filed and no conviction for any offence occurs (provided that the terms of the NPA are satisfied).

Under the terms of a DPA, the government agrees to hold in abeyance a criminal charge that has already been filed in exchange for the defendant's agreement to undertake certain actions. This can include financial requirements, monitoring requirements or other conditions, depending upon the nature of the case. The advantage of a DPA is that, provided the terms of the agreement are satisfied for the designated period of time, the government agrees to dismiss the pending criminal case and no criminal conviction results.

The disadvantage of NPA and DPA agreements is that the facts of the case are never tested by the adversarial system in court. Therefore, the government can make demands and allegations without ever having to prove (or even provide supporting evidence) to establish that a crime actually may have occurred.

66 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

There is no restriction on reporting the existence or terms of a DPA or NPA.

67 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Before entering into any settlement or plea bargain, companies must fully assess the risks and costs associated with trial, which involves a critical and detailed analysis of the underlying facts. If a settlement or plea bargain is the appropriate mechanism to resolve the case, companies must consider the effects on business operations and the possible ramifications for suspension, debarment, exclusion, negative publicity, effect on the company's market valuation, or other collateral consequences that may result. Companies should be aware that a resolution with US law enforcement could prompt investigations in other jurisdictions as well as possible private civil litigation, whether in the United States or abroad.

68 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Corporate compliance monitors are regularly used in the context of negotiated resolutions with the DOJ.

69 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Private civil rights of action are sometimes allowed by statute. For example, securities fraud may give rise to private civil claims. Private litigants generally do not have access to the government's files, particularly any materials in possession of the government that were obtained via grand jury subpoena, since such materials are protected by Rule 6(e) of the Federal Rules of Criminal Procedure.

Publicity and reputational issues

70 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

At the investigatory stage, all matters being investigated by a grand jury are protected from public disclosure. While a company is free to disclose the existence of an investigation if it so chooses, this usually does not happen unless the company decides that the existence of an investigation should be disclosed to shareholders or other parties of interest.

Once a case is before a court, the court record and pleadings in the case are generally available to the public, unless the case is filed under seal. The general view is that court cases should be transparent unless there is a special reason for confidentiality being required.

71 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

Public relations firms are regularly used to assist with corporate messaging strategy. However, careful coordination between public relations firms and counsel is of paramount importance. While a statement may be good for the company from a public relations perspective, that

same statement may be harmful to the company from a criminal law perspective, and such statements may be admissible in the event of a trial or other proceeding on the merits.

72 How is publicity managed when there are ongoing related proceedings?

All publicity should be managed through the company's counsel. Counsel should coordinate and manage media issues in connection with public relations professionals.

Duty to the market

73 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Under securities laws governing US issuers, disclosure would be required if the corporation's prior disclosures about the matter would be misleading without the updated information. Disclosure may also be required if the nature of the settlement triggers affirmative reporting obligations, for instance under SEC Regulation S-K.

Anticipated developments

74 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

A bill that is currently being considered in Congress would shift the basis for insider trading liability from fraud to the wrongful use, gathering or communication of inside information. The bill would make it a violation to trade while in possession of material, non-public information 'if such person knows, or recklessly disregards, that such information has been obtained wrongfully, or that such purchase or sale would constitute a wrongful use of such information'. The bill would also make it a violation for a person 'wrongfully to communicate' confidential information if it was 'reasonably foreseeable' that the recipient, known as a 'tippee', would trade on it.

This year will also bring new cybersecurity laws and regulations. In 2019, at least 45 states and Puerto Rico introduced or considered more than 260 bills or resolutions that deal with cybersecurity. Most of the proposed legislation is intended to protect information held by government or businesses from unauthorised access and defending against attacks to various networks, computers and data.

Appendix 1

About the Authors

Jennifer L Achilles
Reed Smith LLP

Jennifer Achilles is a partner in Reed Smith's global regulatory enforcement group based in New York. Her practice focuses on white-collar criminal defence, securities litigation and internal investigations. Jennifer is regularly ranked as a super lawyer and is an active supporter of diversity initiatives. She defends public and private companies, as well as their officers and directors, in insider trading, market manipulation, fraud, antitrust and Foreign Corrupt Practices Act investigations by the SEC, CFTC, FINRA, DOJ and New York DA's and AG's offices. Jennifer also leads internal investigations in advance of and in connection with government investigations, and counsels clients on co-operation and self-disclosure strategies.

Ama A Adams
Ropes & Gray LLP

Ama A Adams is a litigation and government enforcement partner at Ropes & Gray in Washington, DC. Her practice focuses on international transactions and the US government's regulation of trade and investment. This includes, most notably, export controls, economic sanctions, anti-corruption, foreign direct investment and customs laws and regulations. In addition to advising clients on the application of international trade regulations to their business operations, Ms Adams also assists clients in developing compliance programmes, handling pre- and post-acquisition due diligence, conducting internal investigations relating to potential violations of trade laws and representing clients before the US government agencies in connection with enforcement matters and government inquiries. She advises companies in a range of industries, including the oil and gas, aviation, pharmaceutical, manufacturing, technology, chemical and financial sectors.

Pamela Alarcón
Philippi Prietocarrizosa Ferrero DU & Uría – PPU

Pamela Alarcón is a partner at PPU and an expert in criminal law and compliance. She is also an attorney and consultant in criminal law, corporate criminal law, corruption, crime prevention and compliance, as well as risk analysis in corporate business and criminal litigation. She has an outstanding reputation for managing crises arising from criminal activities within companies, by advising legal representatives, chief executive officers, managers and administrators. She is also a criminal consultant and provides risk analysis in real estate, financial, M&A and infrastructure related matters, among others. She has extensive experience in economic criminal law, as well as corruption and criminal compliance issues.

Pamela has law and political science degrees from Los Andes University, a master's degree in advanced studies of human rights from the Carlos III University in Madrid and a specialist degree in corporate law from Pontifical Xavierian University in Bogotá. She is a former adviser to the Office of the Deputy Attorney General and a professor of corporate criminal law and compliance at various universities in Bogotá.

Stuart Alford QC
Latham & Watkins

Stuart Alford QC is a partner in the London office of Latham & Watkins and a member and former co-chair of the firm's litigation and trial department in London. Mr Alford focuses on economic crime and regulatory matters, leveraging his former experience as one of the UK's leading prosecutors to represent clients in their most critical, high-stakes cases.

From 2012 to 2016, Mr Alford headed the Fraud Division at the Serious Fraud Office (SFO), where he was responsible for many of the UK's landmark white-collar cases. His work focused on investigations in banking and money markets, including the wide-ranging cases involving foreign-exchange benchmarks, a major criminal recapitalisation investigation and the Bank of England's liquidity auctions.

Mr Alford has handled numerous multi-jurisdictional investigations, with a concentration on cross-border US–UK matters. He has supervised case teams prosecuting the LIBOR investigations and trials; led the pre-investigation stages of the foreign exchange manipulation cases and supervised the investigation of liquidity auctions run by the Bank of England during the financial crisis of 2007 and 2008.

He was appointed Queen's Counsel in 2014, while working at the SFO, a rare achievement for a lawyer in public service.

Ami Amin
BCL Solicitors LLP

Ami Amin is an associate whose practice covers both business crime and extradition. She has experience in SFO cases involving allegations of bribery and corruption, and in acting for individuals facing proceedings with an international dimension, particularly in matters relating to the Proceeds of Crime Act 2002.

Before joining BCL, Ami was an associate at a leading London criminal defence firm in its regulatory department. She is an experienced litigator with a background in representing professionals facing disciplinary proceedings.

Anupreet Amole
Brown Rudnick LLP

Anupreet Amole is a partner in Brown Rudnick's white-collar crime and regulatory investigations group. Anupreet has handled sensitive investigations in a wide range of multi-jurisdictional business crime matters, many involving allegations of bribery and corruption, fraud, misuse of confidential information, tax evasion and money laundering. Anupreet has particular experience in advising companies on financial crime compliance policies and procedures, including in the context of M&A deals. Past and present clients include various FTSE 100 companies, senior executives, investment advisory firms, professional services firms and high net worth individuals. In addition, Anupreet is co-leader of the firm's cybersecurity group, advising on legal issues both before and after a data incident. Before joining Brown Rudnick in January 2017, Anupreet was a senior associate at Freshfields Bruckhaus Deringer in London. Anupreet is listed in the 2019 and 2020 editions of *The Legal 500 UK*.

Ilias Anagnostopoulos
Anagnostopoulos

Ilias G Anagnostopoulos has appeared as lead counsel in most of the significant corporate and criminal cases in Greece during the past 30 years and is a professor of criminal law and criminal procedure at the School of Law, National University of Athens. He has extensive experience in most types of business crime, financial fraud, European criminal law, tax and customs fraud, healthcare and procurement fraud, medical malpractice, product criminal liability, environmental liability, compliance, money laundering, corruption practices, anti-competitive practices and cartel offences, anti-terrorism, extradition and mutual assistance. His many publications in Greek, English and German deal with matters of Greek, European and international criminal law, business and financial crimes, reform of criminal procedure and human rights.

He is chair of the Hellenic Criminal Bar Association (since 2013) and a member of the Criminal Law Committee of the Council of the Bars and Law Societies of Europe (chair, 2007–2013), the Criminal Law Experts Commission (Ministry of Justice), the High Legal Council with the Bank of Greece, and FraudNet Commercial Crime Services of the International Chamber of Commerce.

Jodi Avergun
Cadwalader, Wickersham & Taft LLP

Jodi Avergun is the chair of Cadwalader, Wickersham & Taft LLP's white-collar defence and investigations group, based in the firm's Washington, DC, office. Her practice focuses on representing corporations and individuals in criminal and regulatory matters involving, among other things, the Foreign Corrupt Practices Act (FCPA). Her experience in FCPA matters includes directing due diligence reviews in connection with mergers and acquisitions in a number of industries and jurisdictions; designing and implementing robust FCPA compliance policies, systems and training for corporate clients; and counselling clients in voluntary disclosures of FCPA violations. Jodi also advises clients in securities enforcement, healthcare and other white-collar matters, and has successfully represented both companies

and senior executives in internal investigations, matters before regulatory bodies, including the SEC, and civil and criminal matters in federal court.

Jodi was an Assistant US Attorney and senior trial counsel in the US Department of Justice for 17 years. She was recognised in the 2014 edition of *The Legal 500 US* as a 'Key Individual' in the white-collar criminal defence area, and was named one of the 2016 '150 Women in White Collar' by *Corporate Crime Reporter*. Additionally, Cadwalader was named a 'Highly Recommended' firm for FCPA by *Global Investigations Review* in its 2016 rankings of the FCPA Bar in Washington, DC.

Amanda L Azarian
Jenner & Block LLP

Amanda Azarian is an associate at Jenner & Block's London office focusing on investigations, compliance and defence. Ms Azarian has extensive experience in working on a range of government enforcement actions in the United States and United Kingdom, including large, complex matters involving the SFO, NCA, DOJ, SEC and OFAC, with a concentration on economic crime. Her practice includes the representation of both corporates and individuals, conducting and advising on global internal investigations, defending against allegations relating to financial crime and responding to government requests, offering compliance advice including in relation to anti-bribery and corruption, anti-money laundering, and sanctions and developing and implementing tailored compliance programmes, due diligence and risk assessments. Prior to joining Jenner & Block, Ms Azarian worked for the Washington, DC, and London offices of an international law firm. Ms Azarian received her law degree from the Catholic University of America, Columbus School of Law, where she served as a staff member of the *Catholic University Law Review* and interned for the Hon. Heidi Pasichow at the Superior Court for the District of Columbia. She is admitted to practise in both Maryland and Washington, DC.

Kevin Bailey
Brunswick Group LLP

Kevin Bailey is a partner in Brunswick's Washington, DC, office focusing on litigation and crisis communications and related reputational issues. Kevin has spent nearly two decades counselling major corporate clients at reputational crossroads, often against the backdrop of Congressional, SEC or other federal government investigations. Prior to joining Brunswick, Kevin served as BP's head Washington lawyer for over seven years and was a key strategist on the company's response to myriad issues related to the Deepwater Horizon accident in the Gulf of Mexico. Kevin also helped to shape BP's public affairs strategies across the United States and served as a key risk management adviser to executives and members of the board of directors for nearly a decade. Before he joined BP, Kevin practised law at WilmerHale in Washington and represented dozens of major companies before Congress and government agencies and in complex litigation.

Alex Bailin QC
Matrix Chambers

Alex Bailin QC is a barrister with extensive experience in business crime, extradition and media law. He is highly recommended by the legal directories in eight practice areas including business and financial crime, extradition and media law. He was previously a derivatives trader in the City. He has represented and advised a number of corporates and high-profile individuals in business crime cases, including many cross-border cases and those involving parallel civil claims.

Michael Barba
BDO USA, LLP

Michael Barba leads BDO USA LLP's national security compliance practice. Michael has led numerous engagements in transactions involving foreign direct investment and critical infrastructure. He has been appointed as an independent and neutral third-party monitor and security officer reporting directly to the Committee on Foreign Investment in the United States (CFIUS) Monitoring Agencies. He also serves as the independent and neutral third-party auditor of a Tier 1 telecommunications company to assess compliance with CFIUS national security agreement mitigation requirements.

Michael's responsibilities include assessing and analysing national security agreements, interim orders and letters of assurance while developing customised work plans that are approved by the US government.

Michael's responsibilities also extend into BDO's forensic technology services group, where he has more than 20 years' experience in managing complex investigations involving high-tech crime, misconduct and network security incident response. Michael has led BDO's digital forensics and incident response practices in conducting domestic and international investigations affecting the computer networks, resources and intellectual property of numerous Fortune 500 organisations. He received the prestigious High Technology Crime Investigation Association Award for 'The Most Significant High Technology Case' involving public and private sector cooperation.

William P Barry
Miller & Chevalier Chartered

William Barry regularly advises boards of directors, companies and financial institutions on a broad range of issues involving white-collar and securities enforcement, transactional due diligence and compliance with Foreign Corrupt Practices Act, money laundering, economic sanctions and insider trading requirements. Mr Barry guides clients through the complex issues involved in responding to inquiries from domestic and international regulators regarding issues of accounting fraud, foreign bribery, money laundering and other financial crimes. He represents clients faced with the challenge of responding to competing demands in parallel proceedings, such as internal reviews, government investigations and private civil actions.

Milos Barutciski
Borden Ladner Gervais LLP

Milos Barutciski has represented Fortune 500 clients and companies listed on the Toronto Stock Exchange, the New York Stock Exchange, NASDAQ, and European and Asian stock exchanges in anti-corruption, sanctions, export control, cartel, government procurement, money laundering and other regulatory investigations and compliance matters. He has represented clients in investigations by the Royal Canadian Mounted Police, the Canada Border Security Agency, the Competition Bureau, the Ontario Securities Commission and other agencies, including investigations by the US Department of Justice, the US Securities and Exchange Commission and the European Commission. Milos has represented clients in several World Bank corruption investigations and has appeared as counsel before the Bank's Sanctions Committee.

Milos is a founding member of the Task Force on Bribery and Corruption of the Business and Industry Advisory Committee to the OECD in respect of the 1997 Anti-Bribery Convention. He also advised the government of Canada with respect to the drafting of the Corruption of Foreign Public Officials Act. From 1996 to 1999, Milos was engaged by the World Bank to advise on regulatory reform in the Middle East and Africa. He is a member of the executive board of the International Chamber of Commerce. He is called to the bars of Ontario and Quebec.

Claudio Bazzani
Homburger

Claudio Bazzani is a partner and co-head of Homburger's white collar and investigations team and litigation and arbitration practice. He specialises in internal and regulatory investigations and advises corporate clients in compliance matters. He represents clients in investigations by Swiss and foreign authorities as well as in domestic and international litigation and arbitration proceedings.

Claudio Bazzani has more than 10 years of experience in conducting large-scale internal and regulatory investigations. He regularly advises and represents clients in financial market compliance issues and has profound knowledge of the legal and practical challenges Swiss companies face in cross-border matters.

Sara Berinhout
Ropes & Gray LLP

Sara Berinhout is an associate in Ropes & Gray's Boston office and is a member of the firm's litigation department.

Benjamin A Berringer
Clifford Chance US LLP

Benjamin Berringer is an associate at Clifford Chance US LLP, where he focuses on cross-border investigations and complex commercial litigation. Ben represents both corporations and individuals in connection with regulatory investigations before the Commodity Futures Trading Commission, the Department of Justice, and the Securities and Exchange

Commission. Ben also advises on matters arising under cybersecurity, privacy and data protection laws. Ben received his BA from Williams College, his MS in economics from SOAS, and his JD from NYU School of Law.

Eike Bicker
Gleiss Lutz

Dr Eike Bicker is a partner and co-head of the compliance and investigation practice of Gleiss Lutz. Eike advises national and international clients on corporate law and compliance. He is a specialist in strategic compliance advisory and compliance investigations. He has particular expertise in corporate governance issues, board matters and company group law issues.

Eike studied at the universities of Saarbrücken, Freiburg and Cambridge (LLM 2005). He has been with Gleiss Lutz since 2015. Eike was previously a partner at a prestigious compliance boutique firm in Frankfurt. In 2014, Eike took up a lectureship in compliance at the University of Bayreuth. Eike speaks German and English.

Caroline Black
Dechert LLP

Caroline Black is at the forefront of the corporate investigations field, acting as trusted adviser for over a decade to companies and individuals involved in the world's largest and most complex cases. She is a criminal defence lawyer and advises organisations, boards and audit committees on conducting investigations and interacting with relevant national authorities, including the Serious Fraud Office, HM Revenue and Customs and the police (and their overseas equivalents). Ms Black focuses her practice on the investigation and defence of business crimes, particularly matters involving corruption, money laundering, fraud and tax concerns.

She has received awards for training and management and has been recognised by *Global Investigations Review* as part of its 'Women in Investigations' issue, which highlighted 100 remarkable women in this field of law from around the world. *Who's Who Legal: Investigations* 2019 has recognised her as a Future Leader, with clients stating that she is 'impressive in her clear-thinking approach to solving important issues'. Ms Black is described as having 'the ability to keep cool in complex and stressful situations' in *The Legal 500 UK* 2018 and is acknowledged by Euromoney's *Expert Guides* 2019 as an Expert for White Collar Crime in the United Kingdom.

Todd Blanche
Cadwalader, Wickersham & Taft LLP

Todd Blanche is a partner in the white-collar defence and investigations group at Cadwalader, Wickersham & Taft LLP. He served for nearly a decade as an Assistant US Attorney for the Southern District of New York. As co-chief of the White Plains Division, he supervised investigations and prosecutions involving public corruption, securities fraud, bank and wire frauds, Medicare and federal programme frauds, RICO violations, violent crimes, and other criminal violations. He also served as co-chief of the Violent Crimes Unit. Todd has extensive trial experience, serving as counsel in 15 federal jury trials. Todd is a recipient of

the Director's Award from the US Department of Justice for Superior Performance as an Assistant US Attorney.

Todd received his undergraduate degree in political science and interdisciplinary studies from American University, and his law degree, *cum laude*, from Brooklyn Law School, where he was the editor of the *Brooklyn Law Review*. He held clerkships with the Hon. Joseph F Bianco for the US District Court for the Eastern District of New York and the Hon. Denny Chin of the US District Court for the Southern District of New York (both now judges of the US Court of Appeals for the Second Circuit).

Bradley J Bolerjack
Reed Smith LLP

Bradley J Bolerjack is a partner in Reed Smith's global regulatory enforcement group in Chicago, where he focuses on complex criminal law matters including sensitive internal investigations, grand jury investigations, compliance counselling and trial practice. Recent engagements have included investigations or indictments (or both) relating to the Foreign Corrupt Practices Act, commercial bribery, antitrust cartels, healthcare fraud, tax evasion, white-collar fraud and government contracting fraud. Brad has been notably successful in avoiding indictment of numerous high-profile clients even after they have received target status. In cases that are indicted, Brad has obtained outstanding results for many clients, whether through trial or negotiated resolutions. His clients include consumer product, medical device, pharmaceutical, manufacturing and other domestic and international companies, as well as individuals.

Nicolas Bourtin
Sullivan & Cromwell LLP

Nicolas Bourtin is a litigation partner and the managing partner of Sullivan & Cromwell's (S&C) criminal defence and investigations group. His practice focuses on white-collar criminal defence and internal investigations, regulatory enforcement matters, and securities and complex civil litigation. He is one of the coordinators of S&C's FCPA and anti-corruption practice group.

Mr Bourtin has represented individuals, corporations and financial institutions in numerous high-profile matters involving accounting fraud, antitrust, FIRREA, the FCPA, insider trading, money laundering, mortgage orientation and servicing, OFAC sanctions, securities fraud, tax fraud and trading. He has extensive experience in representing financial institutions in parallel regulatory and criminal investigations and representing non-US companies and individuals in connection with US investigations.

Mr Bourtin has conducted numerous jury trials and has argued frequently before the US Court of Appeals for the Second Circuit.

He is frequently recognised as a leading practitioner in the area of white-collar criminal defence.

Mr Bourtin also serves, *pro bono*, on the Criminal Justice Act panel for the Eastern District of New York, representing indigent defendants in federal criminal proceedings.

Mr Bourtin served for four years as an Assistant US Attorney in the Eastern District of New York, where he was involved in investigations, prosecutions and trials involving fraud, corruption, money laundering and other white-collar offences.

Michael Bowes QC
Outer Temple Chambers

Michael Bowes QC specialises in business crime, corruption, civil fraud, financial services and economic sanctions. He acts for corporate clients and senior managers in global investigations and for the SFO, FCA, CMA and Lloyd's of London. He advises companies in respect of US and EU sanctions. He acts for overseas regulators and is instructed in overseas cases as an expert in English law. He is regarded as an expert in civil and criminal 'cross-over' work and is described as 'one of the few specialist criminal practitioners in this area' (*The Legal 500* 2015) and as '[v]ery clever and has wide expertise, so is comfortable with criminal and civil work' (Financial Crime: Corporates, *Chambers 2017*). He is listed as a leading silk in the fields of financial services, financial crime (corporates) and financial crime (London) in *Chambers 2017*, and for banking and finance, business and regulatory crime, and fraud in *The Legal 500*. He is listed in *Who's Who Legal 2016* as an expert in business crime defence. He is a joint head of Outer Temple Chambers. He sits as a Deputy High Court Judge (Queen's Bench Division) and as a Recorder of the Crown Court. He is a Bencher of the Honourable Society of the Middle Temple. He is a trustee of Transparency International UK and a co-chair of the UK Chapter of the International Section of the New York State Bar Association.

Matthew Bruce
Freshfields Bruckhaus Deringer

Matthew Bruce is co-head of Freshfields' global investigations group in London, a member of the corporate crime group and an experienced commercial litigator. Highlighted as one of the world's 40 leading investigations specialists under the age of 40 by GIR and recommended by directories (including being listed as a leading investigations and/or litigation lawyer in *Chambers*, *Who's Who Legal* and *The Legal 500*), Matthew has led a number of major corporate internal and external investigations for blue-chip clients in all sectors arising from allegations of bribery and corruption, fraud, misaccounting and human rights abuses. Recent matters have engaged Asia, the Middle East, former CIS territories and Africa. Matthew has been a partner since 2012.

John D Buretta
Cravath, Swaine & Moore LLP

John D Buretta is a partner in Cravath's litigation department and a former senior official at the US Department of Justice (DOJ). He has represented global companies, boards of directors, audit committees, senior management and general counsels of public and private companies, law firms, and former US and foreign government officials with respect to internal investigations, criminal defence, regulatory compliance and related civil litigation matters. He has handled matters involving the Foreign Corrupt Practices Act (FCPA), anti-trust laws, securities fraud and disclosure regulations, money laundering and anti-money laundering controls, trade sanctions, export controls, cyber intrusion and tax compliance, and has appeared for clients before numerous US enforcement agencies. Mr Buretta served for 11 years in the DOJ, including supervising the Criminal Division, where he oversaw nearly 600 prosecutors in international investigative matters involving corporate fraud, the FCPA, insider trading, healthcare fraud, money laundering, the Bank Secrecy Act, trade

sanctions, asset forfeiture, cybercrime, intellectual property theft and public corruption. He currently serves as an independent monitor in separate appointments by the DOJ and US Department of Transportation.

Matthew Burn
Ropes & Gray LLP

Matthew Burn is a member of Ropes & Gray's litigation and enforcement practice group, based in London. Matthew's practice focuses on corporate and financial crime defence, contentious regulatory matters and internal investigations. Matthew has extensive experience advising both corporations and individuals facing complex cross-border investigations and prosecutions relating to allegations of bribery and corruption, money laundering, fraud and other types of misconduct or regulatory failings.

Matthew was previously seconded to a global financial institution and a leading professional services firm to assist with internal and regulatory investigations.

Matthew joined Ropes & Gray in 2018 from a magic circle firm in London.

Diego Cardona
Philippi Prietocarrizosa Ferrero DU & Uría – PPU

Diego Cardona is a partner at PPU and an expert in antitrust, unfair competition and consumer protection law. He has advised important clients in complex merger control procedures and has acted in some of the most important competition cases in Colombia. He has also participated in many administrative procedures and judicial actions regarding antitrust law, unfair competition and international trade. He was recently designated by the Colombian competition authority as non-governmental adviser for the International Competition Network.

James Carlton
Fox Williams LLP

James Carlton is a partner at Fox Williams LLP specialising in all areas of business crime and regulation. Sources say he 'inspires total confidence from his clients, has a wonderful knack of making them feel comfortable and superbly represented, while not pulling any punches in terms of problems they may face' (*Chambers*, 2017).

James has been instructed in a number of the largest and most complex white-collar investigations and prosecutions brought by the UK regulatory and prosecuting authorities, including the Serious Fraud Office and the Financial Conduct Authority, relating to, among other things, allegations of fraud, money laundering, insider dealing, market abuse, and bribery and corruption. Increasingly these have significant international dimensions and considerations.

James also has great expertise in the conduct of public inquiries. He has been instructed by interested parties in a large number of the highest-profile public inquiries, including, among others, the BSE, *The Marchioness*, Leveson, Pollard and Victoria Climbié inquiries.

He has been instructed on a number of complex and cross-border regulatory investigations for senior executives. He has also been instructed in relation to the regulatory

investigations into the manipulation of LIBOR, EURIBOR and FX. He has extensive experience of high-profile corporate investigations involving complex issues of financial crime, bribery and corruption, employee fraud and significant acts of dishonesty.

Sinead Casey
Linklaters LLP

Sinead Casey is a partner in Linklaters' employment and incentives group in London. She advises on a broad range of employment advisory and regulatory issues, including executive appointments and terminations, internal and regulatory investigations, group reorganisations and restructurings, outsourcings and the employment aspects of public and private M&A deals. She has particular expertise working with clients on crisis management mandates, advising them on their most challenging and sensitive HR-related issues as they navigate their way through a crisis.

Sinead's typical advisory work includes counselling on recruitment and termination, redundancy exercises, employment contracts, policies and procedures, grievance and disciplinary proceedings, the implementation of pension and other benefit changes, trade disputes and corporate governance-related issues.

Sinead represents clients before employment tribunals, the High Court and the Court of Appeal, including in unfair dismissal, discrimination and breach of contract claims.

Sinead has a special interest in diversity and is involved in Linklaters' graduate recruitment programme and various corporate social responsibility programmes.

Lavanyaa Chopra
Law Firm of Panag and Babu

Lavanyaa Chopra is part of Panag and Babu's internationally acclaimed compliance and investigations practice. Lavanyaa's advocacy is primarily focused on matters of financial fraud, bribery, money laundering and failure of internal control mechanisms.

Her experience includes conducting internal investigations into complex financial crimes and defending corporations facing multi-jurisdictional regulatory and law enforcement action.

Lavanyaa sectoral focus is principally financial institutions, which she helps in building robust internal controls and enhancing governance mechanisms.

Eric Christofferson
DLA Piper LLP

Eric Christofferson is an experienced litigation and compliance lawyer in DLA Piper's Boston office and is a member of the firm's white-collar group. He represents corporations and individuals in government investigations, internal investigations, criminal and regulatory proceedings, and civil litigation. Prior to joining DLA Piper, Eric served as an Assistant US Attorney in the District of Massachusetts, primarily prosecuting economic and other white-collar crime. Eric, whose practice focuses on the life sciences and financial services sectors, is an experienced courtroom lawyer who has tried more than 15 criminal and civil jury trials during his career.

Jonathan Cotton
Slaughter and May

Jonathan Cotton is a partner in Slaughter and May's dispute resolution group. He covers a range of cases involving contractual disputes, competition disputes and restructuring and insolvency matters. He also often advises on contentious aspects of corporate transactions, including takeovers.

He is particularly experienced in matters involving allegations of wrongdoing in its various forms. On the civil side, these have included cases involving the 'theft' of confidential information by employees and competitors, conspiracy and civil fraud. On the criminal and regulatory side, he has been involved in investigations and criminal prosecutions, cases concerning cartels, and regulatory cases concerning the Bribery Act, the Proceeds of Crime Act, the Fraud Act, FSMA, export controls and sanctions, and Companies Act offences.

The major investigations and disputes on which he has been engaged span business sectors including telecoms, investment banking, investment management, technology, heavy manufacturing, natural resources and fast-moving consumer goods.

Mark Chu
Herbert Smith Freehills

Mark Chu advises Chinese state-owned enterprises and private enterprises, and multinational corporations operating in China, on contentious matters. His practice focuses on compliance and investigations, international arbitration and US litigation. Mark is qualified in Illinois, United States, and Hong Kong. He is a native speaker of English and is fluent in Mandarin, and is based in Beijing.

Edward Craven
Matrix Chambers

Edward Craven is a barrister with particular expertise in media, criminal and data protection law. He is recommended by *The Legal 500* (2020) as a leading barrister in eight practice areas: media and entertainment; defamation and privacy; data protection; civil liberties and human rights; administrative and public law; environmental law; proceeds of crime; and public international law. He has extensive experience of advising individuals and corporations on a wide range of issues relating to business crime investigations and prosecutions, extradition and mutual legal assistance, reporting restrictions and related reputation management issues.

Gail E Crawford
Latham & Watkins

Gail Crawford is a partner in the London office and chair of the firm's data privacy committee and the global technology transactions practice. Ms Crawford is ranked as a leading individual for data protection privacy cybersecurity by *The Legal 500* (2019). Her practice focuses on advising on data protection, e-commerce and consumer protection legislation, as well as advising on technology, intellectual property and commercial law, including technology and intellectual property licensing agreements, joint ventures, technology procurement and outsourcing.

Ms Crawford is an editor of the Latham & Watkins Global Privacy & Security Compliance Law Blog and General Data Protection Regulation (GDPR) Resource Center.

Tracey Cui
Herbert Smith Freehills

Tracey Cui advises multinational and regional corporates operating in China on investigations and compliance matters, commercial dispute resolution and international arbitration. She has a particular focus on investigations and compliance issues that arise under PRC criminal law and anti-unfair competition law. Tracey has spent time on secondment at multinational corporates advising on anti-corruption investigations and compliance matters.

Tracey has passed the PRC National Bar Exam in 2009. She is fluent in Mandarin and English, and is based in Shanghai.

Christine Cuthbert
Herbert Smith Freehills

Christine Cuthbert is a senior associate in the Hong Kong disputes practice, specialising in corporate crime and investigations. She has extensive experience in all forms of contentious work, including cross-border investigations and litigation, and other corruption-related matters. Christine has been with Herbert Smith Freehills for more than 10 years and has worked in their offices in both Hong Kong and Australia. Her experience includes assisting clients with investigations by local and foreign authorities, internal investigations and corporate compliance, addressing anti-money laundering issues and dealing with other regulatory and enforcement bodies.

Christine is qualified to practise in Hong Kong and Australia (Queensland).

Robert Dalling
Jenner & Block London LLP

Robert Dalling is special counsel in Jenner & Block's investigations, compliance and defence practice group. Previously a criminal barrister, Robert has substantial experience in advising both individuals and corporates on issues including bribery and corruption, money laundering, fraud, benchmark manipulation (including LIBOR and FX), and trade and financial sanctions. As a result of the international nature of his caseload, he has acquired experience of a wide range of regulatory agencies operating within the UK (including the SFO, FCA and PRA), the European Union, the United States, Asia and elsewhere.

Eleanor Davison
Fountain Court Chambers

Eleanor Davison is a barrister at Fountain Court Chambers specialising in cross-border white-collar crime, fraud, corruption and contentious regulatory cases. Consistently recognised as expert in the fields of financial crime, financial crime (corporates), financial services and money laundering, by *The Legal 500* and *Chambers and Partners*, she has recently been described as having 'a phenomenal brain and in-depth knowledge of her area of expertise. She is quick-witted, alert to opposing arguments and a delight to work with – a real star to watch'

(*Chambers and Partners UK* 2019, Financial Crime). The directories also describe her as '[v]ery good and particularly experienced in complex investigations involving financial institutions'. Eleanor was listed in *Who's Who Legal* as a Future Leader in investigations in 2018.

Caroline Day
Kingsley Napley LLP

Caroline Day specialises in serious fraud and financial crime. She represents corporates and individuals in complex global investigations. She has conducted numerous internal investigations on behalf of companies in relation to allegations of financial crime and misconduct, including fraud, theft, corruption, money laundering and environmental crime. She advises companies and individuals who are subject to investigations and prosecutions by various agencies including the Serious Fraud Office, the Financial Conduct Authority, HM Revenue and Customs, the Crown Prosecution Service, and the Competition and Markets Authority. Caroline has a particular interest in cross-border cases and her experience extends to MLA requests and extradition. Caroline has been recognised in GIR's 100 'Women in Investigations 2018', and sits on the executive committee of the Fraud Lawyers Association.

Tapan Debnath
Nokia Corporation

Tapan Debnath is senior legal counsel for Nokia handling ethics and compliance investigations in Europe, the Middle East and Africa and serves as the compliance lead for the Nokia Enterprise Business Group. Prior to joining Nokia in January 2016, Tapan was a prosecutor at the UK's Serious Fraud Office, where he investigated and prosecuted major international economic crime cases. Tapan is an experienced English-qualified solicitor specialising in corporate crime and holds a certificate in financial crime from the University of London.

Rebecca Devaney
Pinsent Masons LLP

Rebecca Devaney is a solicitor at Pinsent Masons LLP and a member of the international white-collar crime, investigation and compliance team. She specialises in the conduct of investigations, self-reporting and anti-bribery compliance, as well as sanctions and export controls.

William H Devaney
Baker McKenzie LLP

William (Widge) Devaney is a partner in Baker McKenzie's North America litigation group in New York, co-chair of the firm's global compliance and investigations group and co-chair of the North American government enforcement practice. He was an Assistant United States Attorney in the District of New Jersey, where he was a member of the Securities Fraud Unit. Widge's main areas of practice are white-collar criminal defence, investigations, compliance and complex civil litigation.

Widge is the author of multiple publications involving such topics as the FCPA, investigations and corporate compliance programmes. He appears often in the print media commenting on current criminal matters.

Widge received an AB and JD from Georgetown University, and an LLM from Cambridge University. He clerked for the Hon. Oliver Gasch on the US District Court for the District of Columbia. He is a member of the New York Bar.

Enrico Di Fiorino
Fornari e Associati

Enrico Di Fiorino is a partner of Fornari e Associati, where he specialises in white-collar crime (serious fraud, tax evasion, bankruptcy, corporate crimes, market abuse) as a criminal defence counsel. He has particular expertise in environmental offences, anti-money laundering and medical malpractice.

Enrico advises companies and individuals in criminal inquiries and represents them in criminal proceedings. He has dealt with cases of criminal, internal and regulatory investigations, as well as representing clients in extradition proceedings and European arrest warrant cases.

Enrico is the author of various publications on environmental criminal law, tax law and corporate law. He frequently participates as a speaker in conferences on criminal law for executives, lawyers and accountants. He is a member of the European Criminal Bar Association, European Fraud and Compliance Lawyers, Extradition Lawyers' Association and International Bar Association.

J Robert Duncan
Cadwalader, Wickersham & Taft LLP

Robert Duncan, an associate in Cadwalader's white-collar defence and investigations group, advises clients in a variety of criminal, civil and regulatory matters, including compliance with the Foreign Corrupt Practices Act, and accounting and reporting regulations.

Prior to law school, Robert was a senior audit, assurance and risk advisory associate at a Big Four accounting firm. He is a licensed certified public accountant in the Commonwealth of Kentucky. Robert has taught undergraduate courses in accounting and auditing at the McIntire School of Commerce at the University of Virginia, where he has been a visiting lecturer and instructor.

Robert received his JD from the University of Virginia, where he served as a senior editor for the *Virginia Law and Business Review*. He earned his MS in accounting from the McIntire School of Commerce at the University of Virginia and his BS in accounting from Ball State University's Honors College. Robert is admitted to practise in the State of New York and the District of Columbia.

Kylie Dunn
Russell McVeagh

Kylie Dunn leads Russell McVeagh's national employment law practice. She routinely deals with regulatory and internal investigations, including providing advice on data protection, employment law and search orders.

Ciara Dunny
Matheson

Ciara Dunny is a senior associate in the regulatory and investigations team within the commercial litigation and dispute resolution practice. She has more than five years' experience in corporate crime and investigations and regularly advises both domestic and international clients on bribery, corruption, fraud, money laundering, investigations and trade sanctions, and related compliance issues. Ciara joined the team in July 2018 from Addleshaw Goddard's London office. Ciara's experience in investigations extends to the United Kingdom, the United States, Europe, China, Korea, the United Arab Emirates and Iran. Ciara also represents clients in large-scale civil litigation, including in relation to civil fraud, product liability, professional negligence and debt recovery. Ciara is recognised as being Most Highly Regarded in Europe in *Who's Who Legal: Investigations – Future Leaders* 2018 and 2019. She is also the only Irish lawyer listed in the Expert Guides *Rising Stars* 2019 in white-collar crime and was shortlisted for Rising Star in Litigation in the Euromoney for Women in Business Law Awards Europe 2019.

Clémentine Duverne
Navacelle

Clémentine Duverne represents foreign and domestic clients. Prior to joining Navacelle, Ms Duverne worked in the white-collar department of a major US law firm.

During the past few years, Ms Duverne has represented clients in OFAC investigations of global institutions based in the European Union conducted by the US Department of Justice, New York County District Attorney's Office, New York State Department of Financial Services, Federal Reserve Bank of New York and Southern District of US Attorney's Office; foreign and domestic financial institutions before French criminal courts in fraud and counterfeiting matters; and individuals of a foreign subsidiary of a French institution in connection with a criminal investigation on charges of money laundering and tax evasion.

Allison Eisen
Cravath, Swaine & Moore LLP

Allison Eisen is an associate in Cravath's litigation department.

Jaime Orloff Feeney
Ropes & Gray LLP

Jaime Orloff Feeney, an associate at Ropes & Gray in Chicago, frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Felipe Noronha Ferenzini
Trench Rossi Watanabe

Felipe Noronha Ferenzini joined the firm in 2009. He has more than 12 years of practice in the field of compliance, administrative law and regulatory, assisting public and private clients in national and multi-jurisdictional operations. Currently, Felipe is a teacher on a postgraduate course on compliance at Ibmec in Rio de Janeiro. He is also an alumnus of the International Anticorruption Academy. Felipe is a certified fraud examiner under the Association of Certified Fraud Examiners. Felipe worked at the London and Mexico offices of Baker McKenzie in 2016–2017. He has experience in compliance, leading complex investigations, implementation of compliance programmes, conducting risk assessment and training. He was one of the coordinators of the independent investigation at Petrobras in connection with Operation Car Wash. He also has significant experience in assisting clients in public procurements, negotiating contracts (including with the government), litigating and liaising with auditing authorities.

Kaitlyn Ferguson
Clifford Chance US LLP

Kaitlyn Ferguson represents clients in white-collar and government investigations and regulatory proceedings, with experience handling anti-fraud, anti-corruption/FCPA and anti-money laundering matters. She has represented clients facing scrutiny from the Department of Justice, Securities and Exchange Commission, and Commodity Futures Trading Commission, and has designed and conducted confidential internal investigations spanning multiple jurisdictions.

Reto Ferrari-Visca
Homburger

Reto Ferrari-Visca is an associate of Homburger's white collar and investigations team and litigation and arbitration practice. He specialises in domestic and international litigation and administrative proceedings. He has broad experience in internal and regulatory investigations and advises corporate clients in regulatory and compliance matters. His practice also focuses on privacy and data protection law and he regularly advises clients on cross-border privacy and data protection issues.

Rod Fletcher
Herbert Smith Freehills LLP

Rod Fletcher practised for more than 30 years in all aspects of white-collar and business crime. He represented both corporate and individual clients under investigation by regulators and prosecutors in many jurisdictions, including the Serious Fraud Office, the Financial Conduct Authority, the Department of Justice, the Securities and Exchange Commission, the Crown Prosecution Service and Her Majesty's Revenue and Customs. His work often involved assisting clients with internal corporate investigations.

Rod led the team advising ICBC Standard Bank plc in relation to the ground-breaking first-ever deferred prosecution agreement entered into in the United Kingdom. The case was

also the first disposal in England of the new corporate offence of failure to prevent bribery under the Bribery Act 2010, and involved a co-ordinated global settlement involving the US Department of Justice and the Securities and Exchange Commission. The case had no precedent and set the template for DPAs in the United Kingdom.

Rod also acted in the global LIBOR and FX investigations, and had extensive experience in cartel investigations and prosecutions, including appellate proceedings in the Supreme Court. He represented clients in the SFO investigations into Rolls-Royce, GSK and Tesco, and a defendant in the SFO prosecution arising from the raising of capital by Barclays Bank from Qatar in 2008.

He passed away in November 2019, after a period of illness.

Jonathan Flynn
BCL Solicitors LLP

Jonathan Flynn is an employed barrister specialising in criminal and regulatory law. He has particular expertise in fraud, bribery and corruption, restraint and confiscation proceedings, and general crime.

Jonathan has acted in a number of high-profile, complex and multi-jurisdictional cases, including investigations or prosecutions by the CPS, the FCA, HMRC, the SFO and the NCA.

Lisa Foley
Dechert LLP

Lisa Foley focuses her practice on white-collar crime and has particular experience in the investigation and defence of matters involving international fraud, money laundering and corruption.

Ms Foley advises organisations and individuals on internal investigations, multi-jurisdictional regulatory investigations, raids and prosecutions undertaken by authorities and regulators such as the Serious Fraud Office, the National Crime Agency and the Financial Conduct Authority.

Héctor Gadea
Rebaza, Alcázar & De Las Casas

Héctor Gadea is a graduate lawyer from the Pontifical Catholic University of Peru. In 2014, he was awarded an LLM by Columbia University, New York. In addition, he holds a master's degree from the universities of Barcelona and Pompeu Fabra (Spain). Héctor is certified by the Society of Corporate Compliance and Ethics as a compliance and ethics professional.

Héctor is a partner at the firm, where he focuses his practice on litigation, white-collar crime and corporate compliance. He is a former criminal law lecturer at the Pontifical Catholic University and the Peruvian Judiciary Academy. He has participated as a speaker at a number of international conferences and events.

João Augusto Gameiro
Trench Rossi Watanabe

João Augusto Gameiro became partner of the firm in 2018. He has more than a decade of experience in criminal law and compliance. As a criminal lawyer, he has represented several multinational companies and their shareholders and directors in police inquiries, criminal proceedings, administrative proceedings and parliamentary committees of inquiry in cases of tax evasion, environmental crimes, consumer crimes, antitrust, corruption, trademark and patent infringement, unfair competition, money laundering and currency evasion. He has also provided legal advice to foreign companies regarding Brazilian criminal law, participated in due diligence projects focused on criminal liability and exposure to anti-corruption and anti-money laundering legislation, and has conducted internal investigations into corporate fraud and competitive violations.

Mr Gameiro holds a law degree (2003) and a master's degree in criminal law (2007) from the University of São Paulo and a postgraduate degree in economic criminal law (2014) from the University of Coimbra. He attended the intensive corporate compliance and ethics course at New York University in 2015.

Sona Ganatra
Fox Williams LLP

Sona Ganatra is a partner at Fox Williams LLP specialising in financial services regulatory investigations and internal investigations. She has extensive experience in advising corporates and individuals on a broad range of regulatory issues, particularly in relation to financial crime (such as money laundering, bribery and corruption, and fraud) as well as issues arising in relation to consumer-credit activities, payment services and e-money. She is regularly instructed in relation to FCA and SFO investigations, prosecutions and enforcement action against corporates and senior individuals. She also has extensive experience of high-profile corporate investigations advising on issues of self reporting to and liaising with a variety of regulatory bodies and prosecuting authorities.

Earlier in her career, Sona was seconded to the Enforcement Division of the Financial Services Authority, where she appeared before the Regulatory Decisions Committee and participated in settlement discussions with financial institutions. This provided her with invaluable insight into regulatory investigations and disciplinary actions.

Sources describe Sona as understanding 'the commercial realities and personal pressures of investigations and proceedings and help[ing] clients manage both' (*The Legal 500*, 2019) and as 'an expert on UK banking regulation' who regularly represents senior executives who are subject to regulatory investigations (*The Legal 500*, 2017).

Tanya Ganguli
Law Firm of Panag and Babu

Tanya Ganguli is part of Panag and Babu's internationally acclaimed compliance and investigations practice. Tanya's advocacy is primarily focused on matters of bribery, corporate governance enhancement and failure of internal control mechanisms.

The core of Tanya's practice is advising multinational companies on matters involving the violation of Indian anti-corruption laws and their interplay with the US Foreign Corrupt

Practices Act, Germany's Criminal Code, the UK Bribery Act, and other foreign legislation dealing with bribery of foreign public officials in India.

Tanya's sectoral focus is manufacturing companies, which she helps in building robust internal controls and enhancing governance mechanisms.

Courtney A Gans
Cravath, Swaine & Moore LLP

Courtney A Gans is an associate in Cravath's litigation department.

Jacob Gardener
Walden Macht & Haran LLP

Jake is an experienced litigator who represents corporations and individuals in criminal, civil and regulatory matters. He has extensive experience managing internal and government investigations, complex commercial disputes, and appeals. He has helped lead internal investigations into high-stakes matters involving alleged violations of the FCPA and securities laws. Jake has also successfully handled numerous civil cases in a variety of areas, including commercial contract disputes, mortgage-backed securities litigation, shareholder derivative actions, bankruptcy and employment law. He has significant courtroom experience, including briefing and arguing several appeals and dispositive motions in criminal and civil cases. Before joining Walden Macht & Haran, Jake clerked for the Hon. Dennis Jacobs of the US Court of Appeals for the Second Circuit and the Hon. Naomi Reice Buchwald of the US District Court for the Southern District of New York. In addition, Jake served for several years as a New York City firefighter. His academic scholarship has been published in the *Journal of Criminal Law and Criminology* and the *Boston University Journal of Science and Technology Law*. Jake is a graduate of Yale Law School and Stanford University.

Laura Gillespie
Pinsent Masons LLP

Laura Gillespie is a partner, qualified in Northern Ireland. Laura has more than 15 years' experience in the jurisdiction. She has particular experience in internal investigations and has been involved in a range of international investigations. Laura also handles civil fraud, complementing her investigation experience. She also regularly helps clients with board-level training and policy implementation.

Hector Gonzalez
Dechert LLP

Hector Gonzalez, the chair of Dechert's global litigation practice and a member of the firm's policy committee, is a Fellow in the American College of Trial Lawyers. He advises corporations and executives on a wide range of matters, with a focus on complex commercial and securities litigation, criminal and related civil and administrative matters, SEC and CFTC enforcement proceedings, and internal, grand jury and state attorneys general investigations. In addition, he regularly represents clients in all aspects of Foreign Corrupt Practices Act (FCPA) matters and has extensive experience in working on matters in Latin America.

Mr Gonzalez has been consistently recognised for his white-collar criminal defence and litigation practices by *The Legal 500: United States*, which praises him as 'a great lawyer', having 'an extraordinary amount of expertise' in securities shareholder litigation, and being 'an excellent trial lawyer and strategic thinker who won't waste clients' time or money'. *Benchmark Litigation* named Mr Gonzalez a Litigation Star for his white-collar defence practice and described him as 'one of the sharpest and most promising talents doing this work right now'. He is also ranked in *The Best Lawyers in America* for his white-collar criminal defence practice.

Mr Gonzalez has significant trial experience, having tried more than 20 federal and state jury trials and argued more than 30 cases before federal and state appellate courts. He was previously an Assistant US Attorney in the US Attorney's Office for the Southern District of New York, where he served as Chief of the Narcotics Unit and was twice awarded the Department of Justice's Director's Award for Superior Performance.

Lara Gotti
Clifford Chance

Lara Gotti is a senior associate in Clifford Chance's litigation and dispute resolution practice based in Perth. Since joining Clifford Chance, Lara has worked predominantly on white-collar and regulatory enforcement matters, with a focus on disputes and clients in the energy and resources sector.

Lara has experience in advising corporations, individuals and boards on regulatory investigations and corporate governance issues such as insider trading, bribery and corruption, tax fraud, misleading and deceptive conduct, unconscionable conduct, false and misleading representations, continuous disclosure, anti-corruption and market manipulation.

Tim Grave
Clifford Chance

Tim Grave specialises in regulatory investigations, commercial dispute resolution and related advice across a wide range of matters, including Corporations Act matters, directors' duties, commercial and contractual disputes, equitable claims, white-collar crime, competition law, sanctions advice, internal investigations and contentious enforcement matters. His experience includes acting for global banks, directors and officers of listed companies, and employees on regulatory investigations. Some recent examples of Tim's experience include acting for the former chairman of an Australian listed entity in ongoing investigations by the Australian Securities and Investments Commission (ASIC) in relation to allegations of foreign bribery; for a director of a publicly listed company in an investigation by ASIC concerning allegations of insider trading; for a company director in a high-profile criminal prosecution for alleged conspiracy to commit insider trading offences; for the chief financial officer of an Australian listed entity in a corruption inquiry; for a global transport company on an internal investigation; for the chief executive officer and managing director of a Forex/contracts for difference provider in an ASIC investigation and related proceedings; and in multiple class actions.

Kelly Hagedorn
Jenner & Block London LLP

Kelly Hagedorn is a partner in Jenner & Block's investigations, compliance and defence practice group. Kelly focuses her practice on white-collar crime, data privacy matters (including data breaches), and international disputes involving fraud allegations. She has particular expertise in matters involving the financial services, gaming, hospitality and outsourcing sectors.

In 2018, Kelly was named in *Global Data Review*'s inaugural '40 under 40' list of up-and-coming professionals working in the field of data law.

Graeme Hamilton
Borden Ladner Gervais LLP

Graeme Hamilton is the national co-chair of BLG's investigations and white-collar defence group. Graeme maintains a trial and appellate practice encompassing commercial litigation, public law and white-collar criminal defence. Graeme has been lead counsel in dozens of trials and contested hearings. He also has substantial appellate experience in both criminal and civil matters. Graeme teaches trial advocacy at the University of Toronto Faculty of Law and previously taught evidence at Osgoode Hall Law School as an adjunct professor. Graeme is well-known to his clients for his strategic focus, exceptional problem-solving skills, entrepreneurial business sense and management skills that build trust and consensus. He has been repeatedly recognised as being at the top of his field by his peers in Benchmark Canada – The Definitive Guide to Canada's Leading Litigation Firms & Attorneys (Future Star), and he is recognised in the 2019 edition of Benchmark Canada 40 and Under Hotlist.

Graeme is a sought-after speaker and author. He has presented in a variety of venues and has published many articles and professional papers. He is called to the Ontario Bar.

John M Hillebrecht
DLA Piper LLP

John M Hillebrecht is the US national co-chair of DLA Piper's white collar, corporate crime and investigations practice. Immediately prior to joining DLA Piper in 2010, John served for 15 years as an Assistant United States Attorney in the Southern District of New York (SDNY), garnering extensive trial, appellate and supervisory experience.

He has served as lead or sole counsel in more than 20 jury trials and approximately 50 Second Circuit appeals. John has represented entities and individuals in the crosshairs of some of the highest-profile criminal investigations of recent years, including the 'expert network' insider trading cases, RMBS fraud prosecutions, the SDNY investigation regarding possible corruption in Governor Cuomo's 'Buffalo Billion' and related development projects, numerous rate-fixing cases (including the LIBOR, FX and ISDAfix manipulation cases), the GM ignition switch case, the ongoing Fiat Chrysler emissions control 'defeat device' investigation, and various FCPA investigations (including the 'Sons and Daughters' DOJ and SEC investigation into banks' hiring practices in China and an ongoing investigation involving one of the world's largest petroleum companies) and False Claims Act matters. He also regularly represents pharmaceutical and medical device companies and individuals in various kinds of investigations.

John is recommended in *The Legal 500 United States* and recognised in *The Best Lawyers in America*. In December 2015, *The National Law Journal* recognised John as one of the top white-collar practitioners in the country.

Louise Hodges
Kingsley Napley LLP

Louise Hodges is the head of the criminal department at Kingsley Napley LLP. She specialises in all fraud and business crime litigation, including investigations and prosecutions by the Financial Conduct Authority, the Serious Fraud Office (SFO), the National Crime Agency, HM Revenue and Customs, the City of London Police and the Crown Prosecution Services. She is head of the Kingsley Napley financial services group and lead partner in the internal investigations team. Louise has a particular interest in cross-border cases representing companies and individuals; in particular she is part of the team representing Tesco in the deferred prosecution agreement with the SFO. Louise is past chair of the Fraud Lawyers Association and former vice chair of the European Criminal Bar Association.

Eugene Ingoglia
Allen & Overy LLP

Gene Ingoglia is a partner in the investigations and litigation practice at Allen & Overy LLP based in New York. His practice focuses on criminal, civil and regulatory securities and anti-corruption matters as well as trial-ready civil litigation. He has extensive experience in handling sophisticated securities and business crime matters and has achieved notable results for a wide variety of clients. He has represented clients in actions and investigations by various US Attorney's Offices, the SEC, the CFTC, FERC, FINRA as well as other US federal and state regulatory agencies in actions and investigations involving allegations of securities fraud, accounting fraud, insider trading, market manipulation, FCPA violations, money laundering, tax evasion, and healthcare fraud.

Previously, Gene was an Assistant US Attorney for the Southern District of New York and a member of the Securities and Commodities Fraud Unit, serving as the lead attorney in numerous federal jury trials and complex white- collar investigations. In that position, he represented the government in the trial and conviction of former SAC Capital portfolio manager Mathew Martoma in the largest insider trading scheme ever charged; led the investigation in the so-called 'London Whale' case alleging the deliberate mismarking of complex securities in order to hide losses and resulting in charges against two former traders at a multinational financial institution; and led the investigation that resulted in the conviction of former bank executives and traders for deliberately overstating the value of certain real estate backed securities in *United States v. Kareem Serageldin*, one of the few successful criminal prosecutions arising out of the financial crisis.

Katrin Ivell
Homburger

Katrin Ivell is a partner of Homburger's white collar and investigations team and the financial services team. She specialises in internal investigations, including when the allegation

relates to sexual harassment or similar misconduct, and advises financial institutions in regulatory and compliance matters. She has conducted monitorships for the Swiss Financial Market Supervisory Authority (FINMA), advised several Swiss banks under the Swiss Bank Programme and is frequently retained by banks in anti-bribery and corruption and anti-money laundering issues.

Andrés Jana
Bofill Mir & Alvarez Jana

Andrés Jana is a founding partner at Chilean law firm Bofill Mir & Alvarez Jana, where he chairs the litigation and international disputes area. He obtained his LLM from Harvard University and graduated *summa cum laude* from the Law School of the University of Chile.

A professor of private law at the University of Chile since 1997, he regularly lectures and publishes on international disputes.

Stacy Keen
Pinsent Masons LLP

Stacy Keen is a specialist in white-collar and business crime. Stacy's areas of expertise include trade and financial sanctions, export controls, bribery, money laundering, and health and safety; in these areas she provides advice on all aspects of investigations, prosecutions, risk management and compliance. Stacy regularly advises oil and gas companies and advanced manufacturers on compliance with Russian and Iranian sanctions, on export controls and on responding to suspected violations of those laws, including the making of voluntary disclosures to HM Revenue and Customs and HM Treasury. She also specialises in compliance with bribery laws, on investigations stemming from corrupt activities and on corporate self-reporting.

Asena Aytuğ Keser
Gün + Partners

Asena Aytuğ Keser has been with the firm since 2011 and is a senior associate. Her practice focuses on dispute resolution, employment, business crime and anti-corruption.

Asena's main area of practice is commercial dispute resolution. She has a specific focus on business crimes and handles various disputes that require the application of both civil and criminal law principles. She advises and represents various multinational companies and their executives with regard to investigations and criminal actions arising from white-collar crimes.

Asena is also experienced in employment law. She provides consultancy and represents clients in relation to a wide range of employment law issues, including preparation and negotiation of employment contracts, personnel management, re-employment and unjust competition actions.

Combining her experience in business crimes and employment law, Asena actively takes part in internal investigation processes of major multinational companies from the beginning, and advises clients on the planning and conduct of the investigation.

Pamela Kiesselbach
Herbert Smith Freehills

Pamela Kiesselbach specialises in corporate crime and investigation matters, as well as disputes. She currently splits her time between Hong Kong and south-east Asia, where she leads teams on some of the largest, and most complex, cross-border internal investigations currently under way anywhere in the world.

She has more than 20 years' experience in assisting multinational and regional clients involved in high-value, cross-border investigations and disputes involving Asian, Australian, European, UK and US companies. Pamela has broad sector experience, spanning energy companies, international and regional investment banks and other financial services providers, transport companies, manufacturers and clients in the technology and telecommunications sectors.

Pamela speaks regularly at conferences in Hong Kong and Singapore and the wider Asia-Pacific region about topics relevant to anti-corruption, cybersecurity, anti-money laundering and corporate crime.

Michelle de Kluyver
Addleshaw Goddard LLP

Michelle de Kluyver is a partner in Addleshaw Goddard's global investigations and contentious regulatory group. Michelle has extensive experience in complex, cross-border financial crime investigations including bribery and corruption, financial sanctions, money laundering and fraud, and also advises clients on related compliance issues. Michelle is also an expert on directors' duties. Michelle is named as a Thought Leader in *Who's Who Legal Business Crime: Defence*. Michelle was selected by *Global Investigations Review* in 2015 as one of 100 remarkable women investigation specialists operating across the world. WWL says: 'Michelle receives widespread plaudits from international peers for her "fantastic" work on cross-border international investigations relating to fraud, bribery and corruption claims.' Michelle and co-author Ben Koehne contributed the chapter on Directors' Duties for the 6th Edition of Sweet & Maxwell's *A Practitioner's Guide to Directors' Duties and Responsibilities*.

Bettina Knoetzl
Knoetzl

Bettina Knoetzl, co-founding partner at KNOETZL, is a leading Austrian trial lawyer with 25 years' experience in Austrian and international high-stakes commercial litigation and business crime matters. She has been a partner in international law firms since 1999 and has tried and resolved hundreds of significant, complex disputes and won important business crime trials for her clients, often under significant media attention.

Bettina specialises in complex litigation, business crime, fraud and asset tracing, compliance and corporate crisis management. Her clients are corporations, multinationals and governments, as well as individuals under their company's protection; her matters usually have complex cross-border aspects. Bettina has been involved in a significant number of internal and external investigations, including investigations under the US Foreign Corrupt Practices Act carried out throughout central and eastern Europe.

For many years, she has been ranked in the top tier by leading international directories, including *Chambers* in litigation and white-collar crime (both Band 1) and is currently

recognised as one of the 10 Most Highly Regarded Individuals in litigation and asset tracing in Europe (*Who's Who Legal*, 2018). In 2017, she received recognition as international Lawyer of the Year in asset recovery (*Who's Who Legal*, 2017).

Bettina is very active in the International Bar Association, for which she chaired the Litigation Committee in 2016–2017. She is president of Transparency International – Austrian Chapter.

Anita Lam
Clifford Chance

Anita Lam is the head of employment, Hong Kong. Anita practises across all areas of employment law, with a particular focus on contentious employment, discrimination and data privacy disputes. As a seasoned litigator, Anita is one of very few solicitors in Hong Kong who has Higher Rights of Audience granted by the Higher Rights Assessment Board.

Sarah Lambert-Porter
Ropes & Gray LLP

Sarah Lambert-Porter is a senior associate in Ropes & Gray's litigation and enforcement practice group, based in London.

Sarah's practice focuses primarily on financial crime including bribery and corruption, terrorist financing, money laundering, fraud, and other misconduct and regulatory failings. She has substantial experience advising financial institutions in relation to internal investigations as well as complex cross-border contentious regulatory matters, and criminal investigations and prosecutions. Sarah also advises in relation to the UK's Senior Managers and Certification Regime.

Sarah was previously seconded to a global financial institution to assist with the design and implementation of controls in relation to the Senior Managers and Certification Regime.

Sarah joined Ropes & Gray in 2018 from a magic circle firm in London.

Margot Laporte
Miller & Chevalier Chartered

Margot Laporte advises global clients facing complex multi-jurisdictional regulatory, litigation, and reputational risk arising from enforcement matters. Her practice focuses on cross-border internal and regulatory investigations, white collar criminal defence, securities enforcement matters, and regulatory compliance, including with respect to the Foreign Corrupt Practices Act, anti-money laundering regulations, economic sanctions laws, insider trading, and accounting fraud. She has represented global public companies, boards of directors, audit committees, financial institutions, hedge funds and senior officers in enforcement matters before numerous US and foreign regulators, including the US Department of Justice, the US Securities and Exchange Commission and the Financial Industry Regulatory Authority, as well as France's Autorité des marchés financiers and other foreign regulators.

Nico Leslie
Fountain Court Chambers

Nico Leslie is a member of Fountain Court Chambers, London.

He was called to the Bar in 2010 and has since developed a practice involving both national and international disputes. In particular, he has done significant work in Singapore, both in arbitration and before the newly formed Singapore International Civil Court.

Nico's practice comprises mainly complex financial and civil fraud litigation, having acted in some of the largest UK disputes of recent years, including the *Sebastian Holdings*, *Algosaibi*, *Gemini* and *Republic of Djibouti* cases. In light of this experience, Nico was recently identified as one of 10 junior 'Stars at the Bar' by the UK legal press.

Nico is the co-author (with Marcus Smith QC) of *The Law of Assignment* (published by OUP), one of the leading texts on the creation and transfer of intangible property. He has also been commissioned by OUP (with Marcus Smith QC) to write a further book: *Private International Law and Intangible Property*. Nico speaks fluent French, Italian and Serbo-Croat, and is comfortable working in those languages.

Megan Y Lew
Cravath, Swaine & Moore LLP

Megan Y Lew is a practice area attorney in Cravath's litigation department. Her practice focuses on internal and government investigations, civil litigation and regulatory compliance, including matters concerning the FCPA, fraud, money laundering and anti-money laundering controls, trade sanctions and export controls.

Richard Lissack QC
Fountain Court Chambers

Richard Lissack QC is a member of Fountain Court Chambers, London.

He is currently and has been repeatedly recognised by all the directories and his peers as a leading practitioner across many disciplines and in particular the law of banking and financial services, regulation and compliance, and white-collar crime.

He was called to the Bar in 1978, and became a Queen's Counsel when aged just 37 in 1994. He is also a QC at the Bar of the Eastern Caribbean, and the Bar of Northern Ireland, and an FLC at the Bar of New York, and most recently became admitted with full rights of audience at the DIFC. He has for over 20 years sat as a judge and as an arbitrator.

His practice is national and international and is currently involved in litigation in London, New York, San Francisco, Abu Dhabi, Dubai, the British Virgin Islands and Switzerland.

His practice comprises mainly high-profile complex litigation and is heavily weighted towards points at which commercial conduct straddles the line between civil, regulatory and criminal law – and in particular cross-border work involving banking and the financial markets.

Richard is co-author of the leading book on the Bribery Act 2010 and also the only post-*Lehman* review of Financial Services regulation in the UK. Both are published by LexisNexis.

He is also consulting editor to OUP's *Public Inquiries*.

Gayle E Littleton
Jenner & Block LLP

Gayle Littleton is a partner at Jenner & Block and a member of its investigations, compliance and defence and litigation practices. She focuses on advising and defending corporations in connection with anti-corruption (FCPA), fraud, whistleblower complaints, #MeToo allegations and regulatory compliance matters; conducting complex, worldwide internal investigations; and defending corporations in connection with civil actions brought pursuant to the False Claims Act and the Financial Institutions Reform, Recovery and Enforcement Act. Before joining Jenner & Block, she served as a federal prosecutor for 12 years, working in the US Attorney's Offices for both the Northern District of Illinois and the Northern District of Florida. She served on the team that investigated and prosecuted former Illinois Governor George Ryan's chief of staff. She also investigated and prosecuted high-level white-collar cases and served as senior litigation counsel to the US attorney, where she advised on charging decisions. She graduated from Cornell Law School and served as a law clerk to the Hon. Joseph L Tauro of the US District Court for the District of Massachusetts and the Hon. Gerald W Heaney of the US Court of Appeals for the Eighth Circuit. She is admitted to practise in New York, Illinois and Florida.

Augusto Loli
Rebaza, Alcázar & De Las Casas

Augusto Loli is one of the main partners of Rebaza, Alcázar & De Las Casas, where he leads the litigation practice area. He has over 20 years of experience as a professional attorney specialising in white-collar crime, compliance and complex corporate litigation. He has designed and implemented the defence strategies of several high-profile criminal cases involving public officials, the financial sector, telecommunications infrastructure, industry and commerce for clients from Latin America, the United States and Europe. He graduated from the National University of San Marcos and completed his master's studies in criminal law at the same university. He is a professor of white-collar criminal law at the St Ignatius of Loyola University and of procedural criminal law at the University of Piura.

In addition to his private practice, he has been consulted several times by government entities, including the Advisory Committee of the Commission of Human Rights of the Congress of the Republic of Peru and the Citizen Security Commission. He is recognised by international legal publications as a leading lawyer and recommended in Peru as an expert within his field.

James P Loonam
Jones Day

James Loonam is a partner at Jones Day in New York City where he regularly advises companies and their senior executives in sensitive investigations. Prior to joining Jones Day, James was an Assistant US Attorney for the Eastern District of New York and Deputy Chief of that office's business and securities fraud section. James graduated from the University Connecticut School of Law with honours, where he was a member of the Law Review.

Rebecca Loveridge
Fountain Court Chambers

Rebecca Loveridge is a barrister practising from Fountain Court Chambers who specialises in all areas of commercial law, including civil and regulatory proceedings relating to financial services. She is regularly instructed on matters concerning privilege and appeared as junior counsel for the Bar Council in *R (on the application of Prudential and another) v. Special Commissioner of Income Tax and another* [2013] UKSC 1 and as junior counsel for ENRC in *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2019] 1 WLR 791. She is also a contributor to the latest edition of *The Law of Privilege*, published by Oxford University Press.

Joanna Ludlam
Baker McKenzie LLP

Joanna Ludlam, a partner in the Baker McKenzie dispute resolution team based in London, leads the market-leading regulatory, public and media law team and co-chairs the firm's global compliance and investigations group.

Joanna advises clients in the areas of corporate investigations, administrative and public law, procurement law and litigation. She has particular expertise in the healthcare, technology and energy, mining and infrastructure sectors. Joanna handles all kinds of high court litigation as well as investigations, including issues of bribery, corruption and fraud. She advises clients, frequently at board level, on regulatory compliance and crisis and reputation management.

Joanna has been recognised by several industry directories and has won numerous awards for her work. She has been named one of *The Lawyer*'s Hot 100 for her practice, recognised by *Who's Who Legal* as a Future Leader of Legal Investigations and described as having an 'excellent reputation within the market', ranked by *Chambers and Partners* with commentators saying 'she is "excellent, knowledgeable and well connected"', and acknowledged by the *Financial Times* as a Champion of Women in the annual FT HERoes awards.

Ben Luscombe
Clifford Chance

Ben Luscombe leads the litigation and dispute resolution practice. He has close to 40 years' experience of representing parties in major arbitrations, major litigation, dispute resolution and advisory and regulatory investigations throughout Australia and Asia. Ben is continuously recognised in leading legal publications, such as *Chambers Global*, *The Legal 500 Asia Pacific* and *Best Lawyers Australia*.

Ben leads some of the highest-profile regulatory, international and domestic dispute cases in the region. In the regulatory space, he has experience in advising a variety of clients on domestic and cross-border regulatory investigations involving insider trading, misleading and deceptive conduct, continuous disclosure, anti-corruption, market manipulation and tax prosecutions.

Michael McGovern
Ropes & Gray LLP

Michael McGovern is co-head of Ropes & Gray's global government enforcement group, concentrating his practice in the areas of white-collar criminal defence and complex civil litigation, with a particular focus on investigations and prosecutions by the US Department of Justice and the Securities and Exchange Commission of alleged violations of the federal antitrust laws, the federal securities laws (including the Foreign Corrupt Practices Act), and alleged violations of various healthcare laws and regulations (including the False Claims Act). Michael has over 25 years of experience representing international and domestic corporations and partnerships, as well as officers, directors and other individual clients in complex criminal and civil investigations and litigation. Michael is listed in *The National Trial Lawyers* Top 100 Criminal Defense Trial Lawyers – New York, *Benchmark Litigation*, *Chambers Global*, *The Legal 500* and *The Best Lawyers in America*.

Prior to joining Ropes & Gray, Michael served for over seven years as an Assistant United States Attorney in the US Attorney's Office for the Southern District of New York, where he held supervisory positions in both the organised crime and terrorism unit and the general crimes unit.

Tara McGrath
Clifford Chance US LLP

Tara McGrath is an associate at Clifford Chance US LLP, where she represents clients in international and domestic white-collar government investigations, and related regulatory and civil proceedings. Her recent representations have involved allegations of securities and accounting fraud, wire fraud and money laundering, in addition to issues of extradition. Tara received her BA from Vassar College and her JD, *cum laude,* from Duke University School of Law.

Neil McInnes
Pinsent Masons LLP

Neil McInnes, partner and barrister, is a criminal defence specialist. He has extensive experience of conducting anti-corruption and related compliance advisory work for European, UK, Asia-Pacific and multinational corporates. He regularly advises clients on the implications of the UK Bribery Act and global anti-corruption trends, as well as on fraud, money laundering and related global regulatory investigations, frequently involving multiple law enforcement agencies around the world. He has been recognised as an expert for a number of years by *Who's Who Legal* in both the business crime corporate defence and investigations categories.

Claire McLeod
Barclays Bank PLC

Claire McLeod is the head of investigations and enforcement for Europe and the Middle East at Barclays. Prior to joining Barclays in 2013 Ms McLeod was at Simmons & Simmons LLP.

Claire McLoughlin
Matheson

Claire McLoughlin is a partner in the commercial litigation and dispute resolution department at Matheson and co-head of the firm's regulatory and investigations group.

Claire has advised a wide variety of clients on contentious matters, with a particular focus on the areas of financial services disputes, contractual disputes and corporate offences. Claire has also been involved in a number of judicial review proceedings, acting both for and against statutory bodies.

Claire is highly experienced in advising clients on all aspects of High Court, Commercial Court and Supreme Court litigation. The majority of Claire's cases consist of High Court and Commercial Court litigation matters. In this regard, Claire has developed experience in case management, disclosure and discovery requirements, including privilege and confidentiality issues, the instruction of experts and procedures relating to preliminary issues and modular trials. From a practical perspective, Claire has particular expertise in coordinating and managing large-scale discovery exercises.

Anthony M Mansfield
Allen & Overy LLP

Tony Mansfield focuses his practice on enforcement defence, civil litigation and regulatory advice involving commodities, securities and related financial derivatives. He regularly represents clients before US and European regulators including the Commodity Futures Trading Commission (CFTC), the Federal Trade Commission, the Federal Energy Regulatory Commission, other federal and state regulatory agencies, the UK Financial Conduct Authority and the European Commission. Tony works with a broad spectrum of market participants, including US and non-US financial institutions, major integrated oil companies, global trading companies, hedge funds, energy marketers, futures commission merchants and exchanges.

Prior to returning to private practice in 2007, Tony served as a chief trial attorney and counsel to the Director in the Division of Enforcement of the CFTC. While there, he managed a team of lawyers and investigators focused primarily on manipulation in the commodities markets. He was responsible for the Division's investigations of numerous energy and power marketing companies relating to price reporting in the natural gas markets. He also played a central role in the Commission's subpoena enforcement actions against natural gas price index compilers, involving First Amendment 'Reporter's Privilege' issues, and was central in the Commission's defence of its exercise of jurisdiction over false reporting in the natural gas markets pursuant to the Commodity Exchange Act.

Tony is a former member of the CFTC's energy and environmental advisory committee and the law and compliance executive committee of the Futures Industry Association.

Sergio Mattos
Rebaza, Alcázar & De Las Casas

Sergio Mattos is a graduate lawyer from the University of St Martin de Porres. In 2017, he was awarded a Chevening scholarship to complete a master of laws degree, with a particular emphasis on criminal justice, at the London School of Economics and Political Science (United Kingdom). He also holds a master's degree, with a specialisation in criminal law, from the University of Seville (Spain), where he also completed his doctoral studies in the same field.

Sergio is a senior associate at the Lima office, where he focuses his practice on litigation, white-collar crime and corporate compliance. He is a former lecturer in criminal law at the Scientific University of the South (Peru). He has also written and published several research articles focused on substantive aspects of criminal law, and he has been a speaker at a number of conferences, both in Peru and abroad.

Max G Mazzelli
Latham & Watkins

Max Mazzelli is an associate in the San Francisco office of Latham & Watkins. He is a member of the firm's litigation and trial department and practises in the area of data privacy, complex commercial litigation, consumer protection and cybersecurity.

Mr Mazzelli represents public and private technology companies in complex commercial and class action litigation in both state and federal courts involving data privacy, consumer protection, and commercial contract disputes. He represents companies in regulatory investigations and inquiries by the Federal Trade Commission (FTC), and other US and global government regulators, agencies and bodies. Mr Mazzelli also counsels technology clients on privacy and internet issues, in particular compliance with CCPA, FTC requirements, GDPR, TCPA, COPPA, BIPA, ECPA and wiretap issues, and CLOUD Act; behavioural advertising and social media; data collection; security incidents; and forensic investigations triggered by government requests for information. Additionally, he assists technology clients with privacy policy drafting and provides transactional support on privacy-related issues.

Francisca M Mok
Reed Smith LLP

Francisca Mok is the managing partner of Reed Smith's Century City office and a member of the global regulatory enforcement group. She represents companies and senior individuals in government investigations by criminal and civil authorities, such as the Department of Justice and Securities Exchange Commission, in cases involving the securities laws, Foreign Corrupt Practices Act and False Claims Act. She also regularly conducts internal investigations for clients in a variety of industries, including internal investigations of alleged violations of company policy and financial fraud, and investigations, pursuant to section 10A of the Exchange Act. Additionally, Francisca handles a variety of complex commercial litigation matters, including in the areas of securities law, unfair competition and class action litigation.

Gustavo Morales Oliver
Marval O'Farrell & Mairal

Gustavo Morales Oliver is a partner at Marval, O'Farrell & Mairal and has been a member of the firm since 2006. He specialises in compliance, anti-corruption and investigations.

He has advised companies from several industries on anti-corruption compliance issues and investigations relating to day-to-day company operations, mergers and acquisitions deals, compliance programmes, complex contracts and cases with the authorities.

Gustavo also has significant experience in corporate, mergers and acquisitions, litigation and cross-border matters.

Before joining the firm, he was in-house counsel in both the private and public sectors. Additionally, in 2010 he was a foreign attorney at Yuasa and Hara Law Firm in Tokyo, Japan.

Gustavo earned a law degree from the Torcuato Di Tella University College of Law in 2001, a specialist degree in finance from the University of San Andrés in 2009, and a master of laws degree (LLM) from the University of Illinois College of Law in 2010. In 2014, he earned the 'Leading Professional in Ethics and Compliance' certification granted by the Ethics and Compliance Officer Association ECOA (USA) and IAE Business School.

He teaches anti-corruption compliance and business law at the Torcuato Di Tella University College of Law. He has published numerous articles and is also a frequent speaker at local and international conferences.

Gustavo is co-director and co-author of the ebook *Tratado de Compliance*, published by Thomson Reuters. He is a member of the Bar of Buenos Aires and of the New York State Bar, and has been recognised by *Chambers Latin America* as a leading practitioner in his field.

Joseph Moreno
Cadwalader, Wickersham & Taft LLP

Joseph Moreno is a partner in the white-collar defence and investigations group at Cadwalader, Wickersham & Taft LLP. He has extensive trial and appellate experience in handling complex investigations and litigation involving the DOJ, the SEC, and other domestic and international law enforcement agencies. Representative matters include money laundering and terrorist financing, cybersecurity and data breach response, securities and accounting fraud, insider trading, bribery (including the US FCPA and the UK Bribery Act), and other white-collar criminal and civil matters.

Joseph served as a trial attorney in the DOJ National Security Division's Counterterrorism Section, was appointed a Special Assistant US Attorney for the Eastern District of Virginia, and served on the FBI's 9/11 Review Commission staff. He has testified before Congress on matters relating to international money laundering and terrorist financing. A decorated combat veteran, Joseph is a lieutenant colonel in the US Army Reserve, has served on active duty as a military prosecutor in Europe, the Middle East and Africa, and was awarded the Bronze Star Medal for his service in Iraq.

Joseph earned a law degree from St John's University School of Law, a master of business administration degree from St John's University Peter J Tobin College of Business, and a bachelor of arts degree from Stony Brook University. He is dual-qualified to practise in the United States and as a solicitor in England and Wales, and is also a certified public accountant. In 2019, Joseph was named a Super Lawyer in DC *Super Lawyers* magazine, and a Future Leader in *Who's Who Legal: Investigations*.

Ben Morgan
Freshfields Bruckhaus Deringer

Ben Morgan is a member of Freshfields' global investigations practice in London and a member of the corporate crime group. Ben joined the firm as a partner in 2017. He advises clients on identifying and controlling the risks that arise from regulatory and criminal law enforcement within the domestic and international landscape. Ben practised as a defence lawyer in the City of London before becoming a board member and the joint head of bribery and corruption at the UK Serious Fraud Office (SFO). There, he led some of the SFO's most significant corporate cases and influenced UK policy matters such as the introduction of deferred prosecution agreements, enforcement of the UK Bribery Act and development of the law of corporate criminal liability. He also had a particular focus on building the international relationships necessary to investigate and conclude the most complex matters.

Christopher J Morvillo
Clifford Chance US LLP

Christopher J Morvillo has extensive experience representing corporate and individual clients in criminal investigations and proceedings, internal investigations, and related regulatory and civil matters. With a particular focus on cross-border government and internal investigations, his many representations have involved allegations of accounting fraud, public and foreign corruption, securities fraud, insider trading, economic sanctions violations, trade secret theft, and computer fraud. Mr Morvillo also advises corporations and businesses on related compliance and policy matters.

From 1999 to 2005, Mr Morvillo served as an Assistant US Attorney for the Southern District of New York, where he investigated, tried and handled appeals in a wide variety of criminal cases, including in the area of healthcare fraud, insurance fraud, money laundering, obstruction of justice, counterterrorism and narcotics. In 2005, he received the US Attorney General's Award for Exceptional Service – the Justice Department's highest award for prosecutors – in recognition of his role in the investigation and successful prosecution of a large international terrorism case.

Mr Morvillo was named one of the top five most highly regarded lawyers in the United States for business crime corporate defence in the 2016 edition of *Who's Who Legal*. Mr Morvillo's expertise has also been recognised by numerous other publications, including *Chambers*, *Best Lawyers in America* and *Super Lawyers New York*. Mr Morvillo speaks and writes frequently on government investigations.

David Murphy
Fox Williams LLP

David Murphy is a partner at Fox Williams LLP who specialises in guiding HR directors, boards and in-house legal teams through difficult employment situations, and in advising senior individuals when they join and leave their employers or face problems during their employment.

His corporate client base is focused on the financial services and professional services sectors, and he is experienced in advising on sensitive investigations in both sectors, particularly in respect of allegations relating to breach of duty, discrimination and harassment. His

individual clients include fund managers, investment bankers, directors of listed companies and lawyers. He has advised several individuals at executive committee level on their departures from a major bank. In 2019, he spoke at the Corporate Compliance and Internal Investigations seminar of the Labour Law Commission and Criminal Law Commission of the Union Internationale des Avocats. In the 2019 edition of *The Legal 500*, David was recognised as providing 'consistently pragmatic and timely advice in a calm and reassuring way'.

Stéphane de Navacelle
Navacelle

With more than 15 years' experience in French and US white-collar crime, Stéphanae de Navacelle has participated in several landmark cases involving the US Foreign Corrupt Practices Act and embargo restrictions (OFAC), charges of market abuse and insider trading, fraud (Forex), benchmark manipulation (LIBOR and EURIBOR), investigations by multilateral development banks (World Bank) as well as criminal and internal investigations in Europe, the Americas and Africa. He advises companies with setting up and auditing ethics and compliance programmes; as such he was appointed as independent compliance monitor and expert pursuant to a negotiated resolution agreement by European groups with the World Bank (2018–2019).

A member of the Paris Bar Council (2017–2019), Stéphane de Navacelle is secretary of the International Committee, of the criminal-prospective subcommittee, a member of the ethics committee on professional secrecy (of which he was formerly secretary) and of the ethics committee on conflict of interest; he has also served as ethics investigator.

Stéphane de Navacelle has been identified as a leading practitioner by *Chambers and Partners*, *The Legal 500 France*, *The Legal 500 EMEA*, *Who's Who Legal* and the Expert Guides for white-collar crime and business crime, investigations and stock market litigation.

Stéphane de Navacelle is a regular participant in seminars and is consulted on issues relating to regulatory and criminal investigations in Europe and the United States.

Jillian Naylor
Linklaters LLP

Jillian Naylor is a partner in Linklaters' employment and incentives group in London with particular expertise in contentious and advisory employment matters. She is described as 'extremely knowledgeable' and 'absolutely brilliant and superb' in her area in *The Legal 500* and *Chambers* directories.

Jillian advises her clients on their most sensitive employee relations issues including whistleblowing and discrimination issues, senior and executive level appointments and terminations, and employment aspects of internal and regulatory investigations, as well as performance, conduct and culture issues that arise within a regulatory environment.

Jillian regularly manages employment litigation in the High Court and employment tribunals as well as using methods of alternative dispute resolution such as mediation and conciliation to resolve disputes. She frequently advises clients on the commercial strategies associated with such processes.

Jillian has considerable expertise advising clients on whistleblowing matters. Jillian is a 'thought leader' in the whistleblowing space and has been involved in leading the firm's

'Listen Up' campaign, which aims to focus the whistleblowing discussions on internal behaviours and responses to whistleblowing. As part of this, Jillian produced an e-Learning module with Protect (formerly known as Public Concern at Work). Jillian is also a regular commentator, blogger and speaker on such issues.

Sheila Ng
Rajah & Tann Singapore LLP

Having developed her legal career in both commercial and criminal litigation since joining the firm as a pupil upon graduation in 2007, Sheila Ng has been involved in a broad spectrum of disputes and advisory work. Her practice focuses on commercial and financial disputes and investigations, fraud and asset recovery, as well as corporate insolvency, and she has broad experience and expertise in these areas.

Sheila has advised and represented various international entities in the investigation and prosecution of cross-border claims involving commercial fraud and breaches of fiduciary duties, and the recovery of assets globally. She has also acted for major international banks and brokerages in investigations into regulatory, risk and compliance issues related to matters such as market manipulation, fixing of benchmark rates, layering and spoofing, and insider trading. She has also been at the forefront of major cross-border insolvencies in the region, having acted and continuing to act for the liquidators of Dynamic Oil Trading (part of the OW Bunker Group), MF Global Singapore and various Lehman Brothers Singapore entities.

Sheila was featured as one of 100 female investigations specialists in Global Investigations Review's Women in Investigations 2018, and was also recently recognised in the 2019 Edition of *Who's Who Legal* as a Future Leader in the field of investigations. Sheila is also a Fellow of INSOL International.

Timothy P O'Toole
Miller & Chevalier Chartered

Timothy P O'Toole has been conducting and leading large-scale defence investigations for over 20 years. His practice's main focus is defending enforcement actions and conducting investigations involving the economic sanctions, export controls and anti-money laundering laws. His clients run the gamut, including US and non-US financial institutions and public companies in the aviation, insurance, logistics, manufacturing, and oil and gas sectors. Ranked as one of the nation's leading international trade lawyers by both *Chambers USA* and *The Legal 500*, Mr O'Toole represents companies and individuals at all stages of the process, including defending enforcement actions brought by the US Department of Justice (DOJ), the Treasury Department's Office of Foreign Asset Control (OFAC), the State Department's Directorate of Defense Trade Controls (DDTC) and the Commerce Department's Bureau of Industry and Security (BIS). He also provides companies and individuals with advice on compliance with the US economic sanctions, export controls and anti-money laundering laws, and interacts regularly with the DOJ, OFAC, the DDTC and the BIS in that capacity. Mr O'Toole has substantial experience dealing with criminal and civil regulators and extensive courtroom experience before judges and juries, having appeared in state and federal courts hundreds of times in a variety of civil and criminal proceedings.

Babajide Ogundipe
Sofunde Osakwe Ogundipe & Belgore

Babajide Ogundipe is the senior partner at Sofunde, Osakwe, Ogundipe & Belgore. He has practised as a commercial litigator in Nigeria for 40 years. His asset recovery practice is part of his practice as a commercial litigator, and he has acted on behalf of numerous clients to assist in the recovery of assets lost as a result of fraud and other misfeasance. He has, as a result, gained enormous experience and has come to be recognised as one of Nigeria's leading lawyers in the field.

He was elected a fellow of the Chartered Institute of Arbitrators in 1994 and served as the chairman of the Nigerian branch from 2006 to 2009. He was the first president of the Lagos Court of Arbitration, from February 2010 to February 2014.

He is a frequent speaker in Nigeria and abroad on arbitration, anti-corruption and asset recovery issues and on the regulation of the legal profession. He is the Nigeria representative for FraudNet (which operates under the auspices of the International Chamber of Commerce) and has served as an officer of the executive of the International Bar Association's anti-corruption and regulation of lawyers' compliance committees.

Olatunde Ogundipe
Sofunde Osakwe Ogundipe & Belgore

Olatunde Ogundipe is an investigator/analyst with Sofunde, Osakwe, Ogundipe & Belgore. He studied law at Essex University and electrical and electronic engineering at Loughborough University. Prior to joining the firm in 2018, he had been conducting investigations on a contractual basis for three years.

Danny Ong
Rajah & Tann Singapore LLP

Danny Ong specialises in complex international investigations and commercial disputes across a multitude of industries. In particular, on the banking and finance front, he has led cross-border investigations involving complex financial products, cryptocurrencies, securitisation transactions, commodities, bonds, market manipulation, insider trading, layering and spoofing, interest rate fixing, currency fixing and money laundering, to name a few. In his role as counsel to liquidators, he has also been called upon to oversee cross-border investigations into the affairs of Lehman Brothers, MF Global Singapore, Dynamic Oil Trading (of the OW Bunker Group) and BSI Bank. Danny also has a very broad experience and is well known for his work in cross-border fraud and asset recovery investigations and litigation. He has been recognised in these areas of expertise by international legal directories, with clients describing him as 'a formidable force', 'an excellent litigator', 'our go-to guy', an 'outstanding lawyer', 'very switched on', 'good when you need someone to fight your corner', 'very commercial, he knows when he has to be aggressive and commercially aware at the same time', and with *Who's Who Legal* ranking him as one of 40 Thought Leaders globally in asset recovery.

Tamara Oppenheimer
Fountain Court Chambers

Tamara Oppenheimer has been practising as a barrister at Fountain Court Chambers since 2002, having previously trained and worked as a solicitor in the litigation department at Allen & Overy. She has a broad commercial litigation practice spanning financial services, regulatory, general commercial disputes, professional negligence, insurance and aviation. She is a contributor to *The Law of Privilege*, edited by Bankim Thanki QC. Tamara is regularly instructed on matters concerning privilege and confidentiality, particularly in the regulatory and investigatory context. She appeared as junior counsel for Eurasian Natural Resources Corporation in two recent privilege decisions, *Dechert v. Eurasian Natural Resources Corporation* [2016] 1 WLR 5027 and *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2017] 1 WLR 4205 (at first instance) and [2019] 1 WLR 791 (CA). She is also acting for the CAA in the forthcoming privilege appeals in *R (on the application of Jet 2.com) v. Civil Aviation Authority* [2018] EWHC 3364 (Admin) and *R (on the application of Jet2.com) v. Civil Aviation Authority* [2019] EWHC 336 (Admin).

Meghan Gilligan Palermo
Ropes & Gray LLP

Meghan Gilligan Palermo is an associate at Ropes & Gray in New York, who frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Sherbir Panag
Law Firm of Panag and Babu

Sherbir Panag is one of India's foremost white-collar crime lawyers and a partner at the Law Offices of Panag and Babu. Sherbir's multidisciplinary white-collar crime practice has been listed and ranked by *Chambers and Partners*, *Who's Who Legal* and *The Legal 500*. He was recently recognised as a 'Thought Leader for Business Crime Defence (Corporates)' by *Who's Who Legal* and *Global Investigations Review* and has been ranked as one of the '40 under 40 Rising Stars of India' by *Legal Era*.

Sherbir has led investigations and acted as defence counsel in some of India's highest-profile cases, which have also had an interplay with law enforcement in the United States, Europe and Asia. These matters have involved allegations of bribery and other misconduct under Indian and foreign anti-corruption laws; financial and regulatory fraud; procurement fraud; violation of sanctions laws; and violation of corporate governance norms. Sherbir's representative experience spans the entire spectrum of courts in India, including the Supreme Court of India.

Sherbir is a senior fellow at the Wharton School's Carol and Lawrence Zicklin Center for Business Ethics Research and a member of Cornell University's – Meridian 180. He also serves on the advisory group of the Deutsche Gesellschaft für Internationale Zusammenarbeit's Alliance For Integrity.

Jessica Parker
Corker Binning

Jessica Parker is a specialist criminal and regulatory litigator with expertise in all areas of business and general crime. Jessica has experience defending against all of the major prosecuting agencies and has represented senior figures in several significant SFO investigations, including Rolls-Royce, Barclays and G4S. Jessica has substantial experience in regulatory matters and frequently advises clients within the financial services industry. She frequently acts in international investigations, including international requests for evidence and asset freezing. In her general crime practice, Jessica has represented a number of high-profile individuals in relation to the most serious criminal charges, from serious assault to drugs offences.

Avni P Patel
Walden Macht & Haran LLP

Avni Patel is an experienced litigator and trial attorney who has represented individuals and corporate clients in complex, sensitive and high-profile cases including in federal, state, and local criminal and regulatory matters. Her practice focuses on white-collar criminal defence, government investigations and regulatory enforcement, and complex litigation. At Walden Macht & Haran, Avni was part of the trial team who successfully defended a corporate client in a high-profile public corruption case in the Southern District of New York. They won the only acquittal in the highly contested and publicised four-defendant trial. She also is part of the WMH team representing one of the most significant whistleblowers in sports history. Additionally, Avni was also on the leadership team of the independent monitor named by the US Department of Justice to oversee General Motors' compliance with its obligations under the deferred prosecution agreement (DPA) stemming from its recall of defective ignition switches. Before joining Walden Macht & Haran, Avni served as an Assistant District Attorney for five years in the Bronx County District Attorney's Office. In those five years, Avni tried over 15 felony and misdemeanour cases to verdict – five of them to jury verdict – on charges ranging from attempted murder to grand larceny. Avni is a graduate of Boston University School of Law and Northwestern University.

Angela Pearsall
Clifford Chance

Angela Pearsall is a partner with more than 20 years' experience in the litigation and dispute resolution practice based in Sydney. Recognised in *The Legal 500* as a 'superb, motivated and hardworking' commercial litigator with financial services as a sector strength, Angela has worked on some of the largest and most high-profile matters in the country. Her areas of specialisation are large-scale commercial litigation, class actions, contentious regulatory disputes and investigations. She regularly represents banks and large corporates in regulatory disputes and investigations. She is recognised as a leading lawyer in the 2016 *Doyle's Guide* and the most recent rankings by *Best Lawyers*.

Angela has significant experience in contentious regulatory matters and has assisted clients with internal investigations and reporting. Her strong client base has included global banks and financial services companies, including HSBC, ANZ, CBA, RBS and BNP Paribas.

Angela has worked on a number of high-profile inquiries, including, most recently, under the Charitable Fundraising Act in relation to various Returned Services League entities and the Banking Royal Commission. She has conducted a number of complex fraud investigations and related litigation.

Nichola Peters
Addleshaw Goddard LLP

Nichola Peters is a partner and heads up Addleshaw Goddard's global investigations and contentious regulatory group. She specialises in advising corporates, directors and senior management on regulatory inquiries, financial and corporate crime issues. Key areas involve advising on and carrying out investigations relating to corporate collapse, corruption, sanctions, money laundering, terrorist financing, extradition, information security and fraud issues. As Nichola regularly investigates compliance failings, she is able to provide specialist non-contentious advice on what to look out for, how matters can go wrong and how to minimise that risk. In relation to contentious matters, because Nichola works regularly with clients to conduct due diligence and implement effective compliance programmes, she has an excellent understanding of industry standard practice and what procedures should have reasonably been put in place to prevent compliance failings. Nichola is ranked as a Thought Leader in *Who's Who Legal: Investigations* and *Who's Who Legal: Business Crime Defence*. Nichola was selected by *Global Investigations Review* in 2018 as one of 100 remarkable women investigation specialists operating across the world. Nichola was also named as one *The Lawyer*'s 'Hot 100' lawyers in 2017.

Hayley Pizzey
Latham & Watkins

Hayley Pizzey is an associate in the London office of Latham & Watkins.

Ms Pizzey's broad practice focuses on multi-jurisdictional litigation and regulatory matters. She advises clients on a wide range of disputes with a particular focus on commercial litigation and contentious data protection as well as regulatory investigations.

Ms Pizzey's experience includes claims in the High Court, the Court of Appeal, and the Competition Appeal Tribunal. She has also acted on matters involving the Competition and Markets Authority, the European Commission, and numerous data protection authorities and financial services regulators across the world.

Glenn Pomerantz
BDO USA, LLP

Glenn Pomerantz leads BDO USA LLP's global forensics practice with nearly 35 years of forensic accounting, auditing and consulting experience. Working with multinational organisations and their counsel, Glenn leads cross-border matters that mitigate the risks associated with fraud and corruption. He works with BDO leaders around the globe to respond to clients' needs involving anti-corruption and fraud investigations, forensic technology, compliance and due diligence matters in mature and emerging markets.

Glenn has significant experience in managing engagements involving alleged violations of the Foreign Corrupt Practices Act and UK Bribery Act, and embezzlement, theft and financial reporting fraud. In addition, he has spent much of his career providing expert witness testimony on economic damages, as well as providing litigation and dispute advisory services, including evaluating claims under fidelity bonds and employee dishonesty insurance coverage. He has also served as a court-appointed umpire and referee and as a neutral arbitrator.

Polly Pope
Russell McVeagh

Polly Pope is one of New Zealand's leading financial, construction and insolvency litigators. She was named as Best Lawyer – Litigation in 2016, 2017 and 2018. She has significant expertise in investigations, originating in the years that she spent in practice at Clifford Chance in London, where she acted on several cross-border internal and regulatory investigations. At the time of writing, Polly was a finalist for NZ Lawyer of the Year (Benchmark Litigation Asia Pacific) and had recently been awarded the prestigious Sir Ronald Davison Award by the Arbitrators' and Mediators' Institute (AMINZ). Polly is a fellow of AMINZ and a member of the Council of the New Zealand Legal Research Foundation.

Charlie Potter
Brunswick Group LLP

Charlie Potter advises a broad range of media, telecoms and professional services clients on many communications issues, particularly in the context of legal proceedings, regulatory disputes, mergers and corporate crises. He co-leads Brunswick's litigation, disputes and investigations practice in London. He is also a partner in Brunswick's family business, crisis and cybersecurity practices. Charlie joined Brunswick in June 2012 from his practice as a barrister at Blackstone Chambers, where he specialised in public/administrative and commercial law, in particular broadcasting and media regulation. During his legal practice, Charlie was regularly instructed by statutory regulators in various proceedings, and advised commercial clients on a range of sensitive regulatory issues. Before the Bar, Charlie spent four years at the BBC, including as a producer at the flagship television news and current affairs programme Newsnight.

Elly Proudlock
Linklaters LLP

Elly Proudlock acts in investigations by the Serious Fraud Office (SFO) and other authorities, representing companies and individuals facing allegations of fraud, bribery and corruption, money laundering and other types of misconduct. Key work highlights for Linklaters include working on an SFO investigation for a multinational energy services company, representing a non-UK listed company in a self-report and acting for a UK listed company in an SFO fraud investigation. Previous experience includes representing senior individuals in SFO investigations involving high profile names such as Barclays, ENRC and Rolls-Royce. Elly also regularly advises companies on the whole range of issues relating to business crime, including anti-bribery and corruption and anti-money laundering. Elly is ranked as 'up and coming' in the *Chambers and Partners* directories for Financial Crime: Corporates.

Nicholas Purnell QC
Cloth Fair Chambers

Nicholas Purnell's practice in commercial and business crime and in regulatory and professional disciplinary matters has spanned over four decades. Typically instructed at the early stages of investigations pre-charge, he advises clients in cases under examination by global regulatory and prosecuting authorities including the Serious Fraud Office (SFO), the Financial Conduct Authority, the US Department of Justice and the Securities and Exchange Commission.

The development of collaborative investigations across jurisdictions has brought about the need for teams to be in place to provide joint advice on the impact of managing the response to investigations on a global basis. Nicholas has specialist experience in the development of the appropriate strategy to enable businesses to develop and cope with the resource demands imposed by such investigations.

Nicholas acted for ICBC Standard Bank throughout the first ever deferred prosecution agreement to be approved in the United Kingdom. Following months of negotiations with the SFO, Nicholas appeared before the President of the Queen's Bench Division at the High Court where the terms of the agreement were finalised. This case marked Nicholas's hat-trick of firsts: the first civil settlement with the SFO for Balfour Beatty; the first attempt at a simultaneous global settlement in the United States and the UK with the SFO in *Innospec*; and the combination of this first charge under section 7 of the Bribery Act in achieving this deferred prosecution agreement with the SFO.

Nicholas successfully represented clients in the United Kingdom over allegations made by the SFO against Tesco and Barclays and advised one of the three DePuy International executives who was on trial in Athens.

Amanda Raad
Ropes & Gray LLP

Amanda N Raad, a US lawyer who is also admitted as a solicitor in England and Wales, serves as co-chair of Ropes & Gray's award-winning global anti-corruption and international risk practice. Amanda has substantial experience negotiating with US regulators on behalf of companies and individuals concerning cross-border matters involving corruption, money laundering and other forms of financial fraud. These matters are often subject to scrutiny by foreign regulators, given their multi-jurisdictional nature.

In addition, Amanda proactively works with clients across industries and geographies to identify and mitigate risk. Finally, Amanda advises clients on corporate social responsibility, supply chain compliance and responsible sourcing. Amanda regularly publishes on cross-border issues and is a frequent speaker at conferences, including on sexual misconduct and investigations. Amanda is listed in Global Investigations Review's *Women in Investigations* 2018, *Chambers UK, The Legal 500 UK* and *New York Super Lawyers*.

Samuel Rabinowitz
Fountain Court Chambers

Sam Rabinowitz is a barrister practising from Fountain Court Chambers and specialising in commercial law. He is regularly instructed on matters in which privilege issues arise, and as a pupil assisted counsel for ENRC in the trial of *The Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation* [2017] 1 WLR 4205. Sam worked as a judicial assistant in the Commercial Court for six months in 2018.

Alberto Rebaza
Rebaza, Alcázar & De Las Casas

Alberto Rebaza is the founding and managing partner of Rebaza, Alcazar & De Las Casas. As partner, he co-leads the mergers and acquisitions and corporate areas. In addition to his master's degree from the University of Virginia, he has studied at Georgetown University and in England.

Alberto has been consistently considered by legal rankings as a leading lawyer in mergers and acquisitions. He has been a speaker at conferences in Dublin, São Paulo, Bogotá, Panama City, Barcelona, New York City, Mexico City and Singapore, among others.

He has been a director for several companies and organisations, such as Edegel (energy), Rigel Peru (insurance), Liderman (services), Amrop (services), IPAE, Pesquera Alexandra (fishing) and YPO.

Very much involved in the arts world, Alberto is vice president of the Museum of Art of Lima, a member of the international patronage committee of the Reina de Sofia Museum and a member of the Latin American Circle at the Guggenheim Museum in New York.

Conor Reardon
Jones Day

Conor Reardon is an associate at Jones Day in New York City. After graduating from the Duke University School of Law in 2014, he served as a law clerk to Judge Robert N Chatigny, of the US District Court for the District of Connecticut, Judge José A Cabranes, of the US Court of Appeals for the Second Circuit, and Chief Justice John G Roberts Jr, of the US Supreme Court. At Jones Day, he focuses on appellate advocacy and critical motions practice, with a particular emphasis on white-collar criminal defence.

Marcus Reischl
Gleiss Lutz

Dr Marcus Reischl is an associated partner and a member of the compliance and investigation practice at Gleiss Lutz. Marcus advises domestic and international clients on compliance, and represents firms in court and arbitration proceedings. He specialises in strategic compliance advice as well as setting up, implementing and developing compliance structures. Marcus regularly assists companies with internal investigations for detecting irregularities, advising on their impact, in particular with regard to judicial and extrajudicial disputes with business partners and co-operation with the authorities.

Marcus studied at the universities of Freiburg (Breisgau), Munich and Passau. He has been with Gleiss Lutz since 2013. In 2012. Marcus worked for an international law firm in Toronto, Canada. He is a member of the Institution of Arbitration e.V. (DIS) and the German Lawyers' Association (DAV). Marcus speaks German and English.

Karen Reynolds
Matheson

Karen Reynolds is a partner in the commercial litigation and dispute resolution department at Matheson and co-head of the firm's regulatory and investigations group.

Karen has a broad financial services and commercial dispute resolution practice. She has more than 10 years' experience in providing strategic advice and dispute resolution to financial institutions, financial services providers, domestic and internationally focused companies and regulated entities and persons. She advises clients in relation to contentious regulatory matters, investigations, inquiries, compliance and governance-related matters, white-collar crime and corporate offences, commercial and financial services disputes, anti-corruption and bribery legislation, and document disclosure issues.

Karen has substantial experience in corporate restructuring and insolvency law matters, having had a lead role in some of the most high-profile corporate rescue transactions of the last 10 years. She advises liquidators, regulators, directors and insolvency practitioners in relation to corporate offences and investigations, shareholder rights and remedies, directors' duties, including in relation to fraudulent and reckless trading, and disqualification and restriction proceedings.

Charles D Riely
Jenner & Block LLP

Charles Riely is a partner at Jenner & Block and a member of its investigations, compliance and defence, markets and trading and securities litigation and enforcement practices. Before joining Jenner & Block, he served as a lawyer at the SEC for more than a decade, most recently as assistant regional director for the SEC's Division of Enforcement. While with the SEC, he worked on matters involving disclosure failures by public companies, alleged fraud and regulatory violations by investment advisers and broker-dealers, insider trading, anti-money laundering violations, 'spoofing' and other forms of market manipulation, failure-to-supervise violations, the adequacy of firms' cybersecurity procedures and protections, and a variety of other fraud and regulatory matters. Mr Riely also coordinated investigations with the US Department of Justice and worked on more than a dozen publicly filed SEC enforcement actions in which criminal authorities filed a parallel case. He graduated from the University of Michigan Law School and served as a law clerk to the Honorable Frank Maas of the US District Court for the Southern District of New York. He is admitted to practise in New York.

Elizabeth Robertson
Skadden, Arps, Slate, Meagher & Flom (UK) LLP

Elizabeth Robertson is a partner in Skadden's government enforcement and white-collar crime group in London.

She advises on multi-jurisdictional business crime and regulatory matters around the world. Ms Robertson has played a role in many of the most important criminal and regulatory investigations in the United Kingdom over the past 20 years, giving her significant understanding of the priorities of the UK prosecuting authorities such as the SFO, the FCA, HMRC, and the Competition and Markets Authority. She has particular experience in corruption, money laundering, economic sanctions and criminal tax cases. Ms Robertson has also advised on criminal cartel matters, and regularly assists with governance and compliance issues as well as proceedings brought by professional and regulatory bodies. She has successfully defended clients on enforcement actions brought by multiple agencies and responded to coordinated dawn raids in the UK and overseas. Ms Robertson also has experience in ancillary matters such as extradition and mutual legal assistance and applying to Interpol for access to information or for information to be amended or deleted.

She is also an accomplished speaker on international business crime.

Flavio Romerio
Homburger

Flavio Romerio is the managing partner of Homburger and heads the white collar and investigations team of the firm. He has extensive experience with the challenges facing Swiss clients appearing before United States courts and regulators.

Flavio Romerio represents clients in investigations by Swiss and foreign government agencies, has led large-scale internal investigations of Swiss clients, and has represented them before Swiss and US regulators, including the US Department of Justice and the Office of Foreign Assets Control. Flavio Romerio regularly advises corporations and their directors and managers on all aspects of white-collar crimes.

Emmeline Rushbrook
Russell McVeagh

Emmeline Rushbrook specialises in commercial and financial dispute resolution, regulatory compliance and enforcement, and public and administrative law. She has extensive experience in advising on regulatory investigations, internal investigations and public inquiries, and regularly advises clients on compliance with New Zealand consumer and financial services laws and on related law reform issues. Emmeline brings a global perspective to her practice, having spent nine years working at Clifford Chance in London. She rejoined Russell McVeagh in 2014 and continues to act frequently on matters that have an international dimension.

Ali Sallaway
Freshfields Bruckhaus Deringer

Ali Sallaway is co-head of Freshfields' global investigations practice in London and a member of the corporate crime group, and she has been a partner at the firm since 2005. With a record of acting on significant cross-border and domestic investigations for clients in all sectors, Ali specialises in particular on corporate and financial crime defence and regulatory enforcement actions. She has significant expertise handling fraud, false accounting, bribery and corruption, money laundering and terrorism matters as well as acting in relation to market abuse, disclosure and listing obligations for listed companies. Highlighted as one of the The Lawyer's Hot 100 for 2015, Ali is recognised as a leading individual in corporate crime, contentious financial services and investigations by all the major directories.

Richard Sallybanks
BCL Solicitors LLP

Richard Sallybanks has been a partner at BCL since 1999 and specialises in complex business crime and regulatory defence work.

Richard has been involved in numerous SFO, FCA, HMRC and CMA investigations and prosecutions, together with associated restraint and confiscation proceedings. His recent SFO experience includes the Alstom, Barclays Qatar and Tesco investigations (acting for senior individuals under suspicion), as well as acting for Robert Tchenguiz in the SFO's Kaupthing Bank investigation (including the successful judicial review challenge to SFO search warrants). Richard has acted in a number of FCA criminal and regulatory investigations for brokers, traders and senior executives, including in relation to allegations of insider dealing and market abuse. He is experienced in cartel investigations, both domestic investigations conducted by the CMA and cross-border antitrust investigations (including those conducted by the US DOJ). Richard is also experienced in the international mutual legal assistance regime, and in leading and co-ordinating teams of lawyers in multi-jurisdictional investigations.

Sandrine dos Santos
Navacelle

Before joining Navacelle, Sandrine dos Santos worked in an elite French litigation boutique and at the Paris Prosecutor's Office from 2007 to 2010. She dealt with cases relating to economic and financial crime or organised crime and damage to persons or property, and acquired a strong expertise in white-collar crime.

Ms dos Santos has worked on complex international corruption matters involving high-profile political stakeholders and large-scale companies in Africa and South America. She also handled sensitive LIBOR-related matters.

Ms dos Santos has assisted clients in setting up global compliance training. She is a regular participant at conferences organised by the French Institute for Higher National Defence Studies.

David Sarratt
Debevoise & Plimpton LLP

David Sarratt is a partner in Debevoise's litigation department. He is a seasoned trial lawyer whose practice focuses on government enforcement actions, internal investigations and complex civil litigation for financial institutions and other clients. Mr Sarratt has particular experience in matters relating to compliance with the Bank Secrecy Act and the Foreign Corrupt Practices Act, as well as with novel enforcement issues arising from new technologies. Prior to joining the firm, Mr Sarratt served as an assistant United States attorney in the Eastern District of New York. As a federal prosecutor, Mr Sarratt supervised and participated in a wide variety of investigations and prosecutions, involving international terrorism, cybercrime, financial and healthcare fraud, racketeering and other crimes. He successfully tried numerous cases to verdict and briefed and argued appeals in the US Court of Appeals for the Second Circuit.

María Lorena Schiariti
Marval O'Farrell & Mairal

María Lorena Schiariti is a partner in the regulatory and administrative law team and the compliance, anti-corruption and investigations team.

In view of the wide variety of international clients subject to the US Foreign Corrupt Practices Act or the UK Bribery Act, she has focused on advising on issues relating to public ethics, anti-corruption, transparency policies and investigations.

Ms Schiariti holds a law degree with a specialisation in administrative law from the University of Buenos Aires, Argentina (1997) and attended the master's in law and economics course at the Torcuato Di Tella University, Argentina (2001–2002). She is currently a professor on the postgraduate course in compliance organised by the Austral University and the Business Institute of Argentina.

She received the Client Choice Award, Public Law (International Law Office, 2018) and she has been listed by *Chambers and Partners Latin America* as a Leading Individual (2009–2019), as a Leading Lawyer by *The Legal 500* (2012–2019) and as Approved Administrative Law Private Practitioner by *LACCA* (2014–2019). She was also included in the list of corporate lawyers to know and compliance lawyers to know by *Latin Lawyer* (2014), *100 Women in Investigation* by *Global Investigation Review* (2015) and as one of the 40 best Argentine lawyers under 40 by *Latin Lawyer* (2003).

Kirsten Scott
Clifford Chance

Kirsten Scott is a counsel in the litigation and dispute resolution practice based in Perth. She specialises in regulatory matters, including white-collar crime, investigations and enforcement, and directors' duties. Prior to joining Clifford Chance, Kirsten worked for the Commonwealth Director of Public Prosecutions Office for more than 10 years in a variety of Australian jurisdictions specialising in commercial and taxation crime. Her work included acting as a senior assistant director for the Commercial Prosecutions branch in Western Australia. This experience gives Kirsten a unique insight into the operation of government agencies and regulatory frameworks.

Kirsten sits on the Law Society of Western Australia's Criminal Law committee and the Competition and Consumer Committee of the Law Council of Australia.

Most recently, Kirsten has advised corporations, individuals and boards on regulatory investigations such as insider trading, misleading and deceptive conduct, continuous disclosure, anti-corruption and market manipulation, including providing advice on corporate governance issues.

Kirsten is regularly retained by individuals, boards and corporate entities in relation to criminal allegations of insider trading and has been involved as an adviser in some capacity in the majority of market-related, contested white-collar criminal matters before Australian courts in recent years.

Kirsten is also the secretary for the Australian Chapter of the Women's White Collar Defense Association.

Judith Seddon
Ropes & Gray LLP

Judith Seddon specialises in white-collar crime, fraud, corruption, and regulatory and criminal investigations and prosecutions. She has deep experience and expertise in advising corporates, financial institutions and individuals in complex investigations and prosecutions, domestically and cross-border, as suspects and as witnesses. She has worked, and is working, on some of the most complex and high-profile investigations and prosecutions. Judith is consistently ranked as a band 1 leading practitioner by *The Legal 500* and *Chambers*. *Who's Who Legal* 2018 named Judith Business Crime Lawyer of the Year and lists her on a shortlist of 10 Thought Leaders. *Who's Who Legal* describes her as 'one of the most highly regarded investigations lawyers in the United Kingdom, highlighted for her "brilliant" work on behalf of both corporates and individuals'.

Sean Seelinger
Ropes & Gray LLP

Sean Seelinger, counsel at Ropes & Gray in London, frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Pedro Serrano Espelta
Marval O'Farrell & Mairal

Pedro Serrano Espelta is a partner at Marval, O'Farrell & Mairal and has been a member of the firm since 1997. He is the head of Marval's compliance, anti-corruption and investigations practice and has led numerous local and international investigations in the field, including asset tracing and recovery cases. He also has extensive experience in corporate law, mergers and acquisitions, and oil and gas.

As the Argentine representative to the International Organization for Standardization in 2016, he participated in the preparation of the Anti-Bribery Management standard 37001.

Pedro received his law degree from the National University of the Littoral in 1992. He was a visiting scholar at the University of California at Berkeley from 1993 to 1995 and received a master of laws degree (LLM) from the University of California, Los Angeles, in 1997.

He was foreign associate at the law firm The Americas Law Group in San Francisco, California, from 1993 to 1996, where he worked on complex international agreements.

Pedro is a frequent writer in specialist publications and a regular speaker at international conferences and seminars on issues relating to his expertise.

He is a member of the Buenos Aires Bar Association and is ranked by *Chambers Latin America* as a top practitioner in the field.

Gabriel Sidere
CMS Cameron McKenna Nabarro Olswang LLP SCP

Gabriel Sidere is the managing partner of the CMS office in Bucharest and head of the dispute resolution and white-collar crime practice in Romania.

Gabriel advises on complex criminal disputes, particularly those relating to fighting corruption and fraud. He also regularly advises on forensic investigations concerning criminal law and regulatory matters. His recent cases include securities regulatory inquiries (market manipulation, insider trading, etc.), and investigations by Romania's anti-corruption agency (DNA) and the organised crime and terrorism investigation agency (DIICOT). For many years, Gabriel has assisted publicly listed companies to conduct internal investigations into allegations of wrongdoing. These investigations have been in a wide variety of industries, including energy, financial services, healthcare and infrastructure.

Gabriel's litigation practice includes the representation of clients in complex business litigation and international arbitrations matters. These representations include strategic advice on investment-related disputes, helping clients manage responses to government inquiries and representing clients in high-level negotiations. Gabriel has successfully argued motions on bilateral investment treaty claims before the International Centre for Settlement of Investment Disputes, a member of the World Bank Group.

Gabriel is an accredited mediator and certified advanced negotiator with the Centre for Effective Dispute Resolution, and has been a member of the Bucharest Bar Association since 1997.

Diego Sierra
Von Wobeser y Sierra, SC

Diego Sierra is head partner of the bankruptcy and restructuring and anti-corruption and compliance practices of Von Wobeser y Sierra. He has more than 15 years of experience and frequently acts as counsel in complex commercial litigation and commercial arbitration disputes. Diego represents several national and international clients in the resolution and prevention of commercial disputes. He has advised global Fortune 500 companies and financial institutions in the United States and Mexico in investigations under the US Foreign Corrupt Practices Act and due diligence matters.

Grace C Signorelli-Cassady
Jenner & Block LLP

Grace Signorelli-Cassady is an associate at Jenner & Block focusing on investigations, compliance and defence. Her experience includes assisting corporates in responding to government enquiries, including by US and European enforcement authorities, assisting corporates in conducting complex, worldwide internal investigations, including in connection with allegations of money laundering, bribery and corruption, and representing individuals in white-collar matters, including for misrepresentations to investors and mail and wire fraud. She has also drafted six *amicus curiae* briefs regarding white-collar and criminal law issues, five of which were filed with the US Supreme Court. Prior to joining Jenner & Block, Ms Signorelli-Cassady served as a law clerk to the Hon. Roslyn O Silver of the US District Court for the District of Arizona, during which time she assisted with matters taken by designation in the US Court of Appeals for the Ninth Circuit. Ms Signorelli-Cassady received her law degree from Harvard Law School, where she was the managing editor of the *Harvard Journal on Legislation*, selected as a criminal justice fellow and trained in negotiation techniques, eventually helping to teach negotiation strategy to executives from around the world in connection with the Harvard Negotiation Institute. She is admitted to practise in Illinois.

Daniel Silver
Clifford Chance US LLP

Daniel Silver is a partner at Clifford Chance US LLP, where he focuses on regulatory enforcement and white-collar criminal defence. Dan represents both individuals and corporations in matters before the Department of Justice and other federal and state enforcement agencies, and counsels clients on risk mitigation strategies with respect to cybersecurity, anti-corruption, sanctions and anti-money laundering issues. Prior to joining Clifford Chance, Dan spent 10 years as a federal prosecutor, serving in several senior leadership positions and overseeing the national security and cybercrime unit within the United States Attorney's Office for the Eastern District of New York. Dan received his undergraduate degree from Brown University and his JD, *magna cum laude*, from NYU School of Law.

Christoph Skoupil
Gleiss Lutz

Dr Christoph Skoupil is an associated partner and a member of the compliance and investigation practice at Gleiss Lutz. Christoph advises companies on all aspects of white-collar crime and compliance. He specialises in defending companies and advising them in cases of criminal offences against the corporation. This includes both internal investigations and preventive measures.

Christoph studied at the University of Mainz. He joined Gleiss Lutz in 2015. From 2013 to 2015, Christoph worked at a leading boutique law firm specialising in white-collar crime. From 2010 to 2012, he lectured in criminal law at the University of Mainz. Christoph speaks German and English.

Nicole Sliger
BDO USA, LLP

Nicole Sliger is a partner in the New York office of BDO USA, LLP with nearly 20 years' experience providing accounting services to private and publicly traded businesses. She assists organisations and their counsel with matters involving alleged financial statement irregularities, management fraud and compliance issues, as well as investigating fraud perpetrated by rogue employees. She also provides monitoring and oversight services to companies required to comply with settlement terms and corporate compliance programmes.

Nicole was the primary project leader for the National Mortgage Settlement engagement, assisting the monitor in evaluating large financial institutions' compliance with the new mortgage servicing rules and other settlement terms. She has been involved in a number of securities litigation matters, monitorships, white-collar crime, investigations and financial statement fraud cases, helping counsel evaluate and interpret auditing, accounting, financial reporting and compliance issues.

Nicole has managed significant corporate investigations for Fortune 500 companies across various industries. She assists counsel in identifying relevant documents during discovery and preparing for depositions of witnesses concerning testimony that involves the application of GAAP and GAAS. She supervises large-scale electronic document reviews and drafts reports used in filings with the US Securities and Exchange Commission and other regulators. She has also led a number of internal and shadow investigations and matters involving whistleblower allegations.

Andrew Smith
Corker Binning

Andrew Smith specialises in business crime, including SFO, NCA and police investigations relating to fraud, bribery/corruption and money laundering, as well as regulatory inquiries brought by the FCA into market abuse and market misconduct. Andrew also regularly acts for individuals facing extradition to a range of countries and provides related advice on Interpol and criminal mutual legal assistance. Case highlights include: acting for individuals in SFO investigations, including Tesco, BAT, Petrofac, Unaoil, LIBOR and EURIBOR; representing a defendant in the FCA's largest prosecution of insider dealing (Operation Tabernula) and FCA regulatory investigations concerning LIBOR and FX; advising businesses on alleged breaches of export controls and trade and financial sanctions; acting for executive counsel to the Financial Reporting Council on disciplinary investigations into major firms of accountants; and representing Shrien Dewani in the South African request for his extradition for the offence of murder.

Meghan K Spillane
Goodwin

Meghan Spillane, a partner in Goodwin's securities litigation and white-collar defence group, focuses her practice on white-collar criminal defence, corporate internal investigations, and complex business and financial litigation. Her experience includes federal criminal and civil investigations, securities class actions and derivative suits, SEC actions, and complex civil litigation matters. In addition to her other client work, Ms Spillane represents indigent criminal

defendants on a *pro bono* basis in a variety of state and federal matters. Ms Spillane is a member of the bar of the State of New York and is admitted to practise before the US District Court for the Southern District of New York. Ms Spillane was named as a 2018 Law360 Rising Star in 'White Collar', was recognised in Who's Who Legal's *Investigations 2019 – Future Leaders* and has been named consistently by *New York Super Lawyers* as a leading white-collar defence practitioner from 2015 to 2019.

Christian Steinle
Gleiss Lutz

Dr Christian Steinle is a partner and co-head of the compliance and investigation practice of Gleiss Lutz. Christian has considerable experience in European and international antitrust law and compliance investigations. He focuses on cartel cases and private antitrust litigation, merger control, online and distribution antitrust law, antitrust compliance programmes and internal investigations.

Christian studied in Tübingen, Fribourg (Switzerland), Bonn and Speyer. He has been a partner at Gleiss Lutz since 2008. In 2004, he was seconded as in-house counsel to a multinational group, where he specialised in international antitrust litigation. He is a member of the Association for the Study of Antitrust Law, the International Bar Association (IBA) and the American Bar Association, and belongs to the IBA Merger Working Group. Christian speaks German, English and French.

Tom Stocker
Pinsent Masons LLP

Tom Stocker is a partner. He specialises in advising businesses on corporate criminal law, regulatory enforcement, internal investigations and compliance. Tom is qualified in Scotland and England and Wales and is ranked in Band 1 by *Chambers and Partners* for corporate crime and investigations (Scotland) and by *The Legal 500* for criminal fraud (Scotland). He has a particular specialism in corporate investigations by Police Scotland and the Crown Office and Procurator Fiscal Service, and in the operation of Scotland's corporate self-reporting and civil settlement regime. He also defends companies and individuals in regulatory enforcement cases brought by the likes of the Gambling Commission, Financial Conduct Authority, HM Revenue and Customs, Ofgem, Office of Financial Sanctions Implementation, and Health and Safety Executive.

Chris Stott
Ropes & Gray LLP

Chris Stott is a member of Ropes & Gray's litigation and government enforcement practice group, based in London. Chris focuses his practice on criminal, contentious regulatory and internal investigations.

Chris has more than 10 years' experience in advising and representing individuals and corporations in connection with investigations and prosecutions by criminal and regulatory enforcement authorities in the United Kingdom and numerous other jurisdictions.

Chris also assists clients with designing and implementing effective compliance and governance arrangements to anticipate and respond to regulatory change.

Chris was previously seconded to a multinational bank to advise the bank and senior executives on its Senior Managers and Certification Regime implementation programme.

Chris joined Ropes & Gray in 2018 from a magic circle firm in London.

Richard M Strassberg
Goodwin

Rich Strassberg, chair of Goodwin's white-collar crime and government investigations practice and a former member of the firm's executive committee, specialises in white-collar criminal defence, SEC enforcement proceedings, FCPA compliance and investigations, internal investigations, and complex business and financial litigation. Mr Strassberg is a Fellow of the American College of Trial Lawyers, one of the premier legal associations in America. He has twice been recognised by *The American Lawyer* as 'Litigator of the Week' as a result of his securing extraordinary victories in some of the most closely followed white-collar trials in the country. He is also acknowledged by his peers as being one of the finest white-collar attorneys, twice being cited in Law360 by white-collar partners at other firms as being the white-collar lawyer that impressed them, or that they most feared to go up against in court. Mr Strassberg is consistently ranked in Band One by *Chambers USA* as among the top New York-based white-collar defence lawyers, is rated as being among the Top 100 lawyers in New York by *New York Super Lawyers* and is regularly included in *The Best Lawyers in America* and other surveys of the top white-collar litigators in the country. Mr Strassberg co-authors a quarterly column on Federal Civil Enforcement in the *New York Law Journal*, authored a chapter in the book *Beyond A Reasonable Doubt*, has published numerous articles in various legal periodicals, including several on the FCPA, has been a legal commentator on numerous programmes, including NPR, Fox News, Dateline and the Financial Management Network, and has been a guest speaker for various organisations, including the American Bar Association, the New York Council of Defense Attorneys, and the Federal Bar Council. Prior to joining the firm, Mr Strassberg was the Chief of the Major Crimes Unit in the US Attorney's Office for the Southern District of New York, responsible for supervising approximately 25 Assistant US Attorneys in the prosecution of complex white-collar criminal cases.

Eric H Sussman
Reed Smith LLP

Eric Sussman is a partner in Reed Smith's global regulatory enforcement group based in Chicago; his practice focuses on white-collar criminal defence and complex internal investigations. Eric was a deputy chief in the Financial Crimes and Special Prosecutions Unit of the United States Attorney's Office in Chicago for more than nine years and recently served as the first assistant state's attorney for Cook County. In more than two decades of practice, Eric has tried more than 35 federal and state cases, briefed and argued multiple appeals before the US Court of Appeals, and directed hundreds of investigations. Eric has handled numerous complex civil and white-collar criminal matters for corporations and executives in courts throughout the United States. Specifically, he has directed internal investigations involving the Foreign Corrupt Practices Act, the False Claims Act, insider trading issues, Dodd-Frank whistleblower provisions and healthcare fraud allegations.

Lisa Tenorio-Kutzkey
DLA Piper LLP

Lisa Tenorio-Kutzkey (LT-K) focuses exclusively on white-collar matters in all phases of US federal government prosecution and investigation, with a focus on criminal antitrust defence, FCPA and complex internal investigations.

Lisa is a leader of DLA Piper's global cartel practice, a former trial attorney with the US Department of Justice's Antitrust Division and a former Special Assistant US Attorney for the US Attorney's Office for the Northern District of California. Fortune and Global Fortune 100, 200 and 500 companies and their executives routinely turn to Lisa for assistance in price-fixing, bid rigging and market allocation conspiracy matters. For more than a decade, she has successfully prosecuted or defended clients in nearly every major criminal cartel investigation by the Antitrust Division. Lisa has represented companies and individuals in a variety of sectors, including the automotive, aircraft and ocean transportation, telecommunications, semi-conductors, pharmaceuticals, construction, chemicals, industrial products, real estate and technology, and other electronic components industries.

In addition, Lisa has extensive experience in all facets of FCPA investigations, defence and compliance. She has directed and conducted cross-border investigations of FCPA and other anti-corruption and related compliance matters. Her practice is global in scope, with experience in Argentina, Belize, Brazil, Canada, Chile, China, Costa Rica, Ghana, Honduras, Hong Kong, India, Korea, Mexico, the Philippines, Russia, Thailand and Venezuela.

Femi Thomas
Nokia Corporation

Femi Thomas is vice president and global head of ethics and compliance investigations at Nokia. Femi is a US-qualified attorney who prior to joining Nokia in April 2017 worked in the white-collar and regulatory enforcement practice at Crowell & Moring LLP, Washington, DC, and then at Weatherford International in both legal and compliance roles and executive business roles. Femi has a *juris* doctorate degree and holds an executive MBA from the University of Oxford.

Olga Tocewicz
Pinsent Masons LLP

Olga Tocewicz is a senior associate specialising in white-collar crime and corporate defence. Olga has extensive experience in advising both companies and senior individuals subject to investigation or prosecution by the UK's major law enforcement agencies in relation to allegations of financial crime, including fraud, insider trading, bribery and money laundering. Olga also provides advice in relation to the implementation of effective compliance programmes and delivers training on the topic.

Luke Tolaini
Clifford Chance

Luke Tolaini is a partner in Clifford Chance's international investigations practice. He has over 20 years' experience of investigations – many of these matters involving cross-border

enforcement and related litigation. His domestic focus has been on matters involving the UK's Serious Fraud Office, Financial Conduct Authority, and the Competition and Markets Authority – including negotiating one of the five DPAs agreed to date in the United Kingdom – while his international practice has frequently involved engaging with US, European and Asian authorities on matters involving corruption, fraud, cartels, money laundering and market irregularities. He is also a lead partner in Clifford Chance's risk team, advising clients on the management and prevention of business conduct risk and crisis management. He is a member of the editorial board of *Global Investigations Review*.

Anne M Tompkins
Cadwalader, Wickersham & Taft LLP

Anne M Tompkins is a partner in Cadwalader's white-collar defence and investigations group, resident in the Charlotte, North Carolina, and Washington, DC, offices, and a member of the firm's management committee. Her practice focuses on representing companies and financial institutions, as well as their officers and directors in criminal, civil and administrative investigations. Anne has extensive experience in crisis management, internal investigations and enforcement matters across a variety of industries, including financial services, higher education and government contracting.

Anne was the United States Attorney for the Western District of North Carolina from April 2010 to March 2015. She led numerous high-profile, complex criminal and civil investigations during her tenure, including a public corruption case involving the former mayor of Charlotte, the national security case against former general and CIA director David Petraeus, numerous securities and financial fraud cases, and significant matters in the mortgage-backed securities business.

Prior to her recent service as US Attorney, Anne was a partner in the white-collar defence practice of a national law firm. In over 20 years' experience in government and private practice, Anne has tried more than 30 cases to verdict, and successfully represented clients in, among other matters, investigations involving the mortgage practices of a national homebuilder, Medicare reimbursements to a cardiac care hospital, and anti-kickback and reimbursement compliance at a national dialysis services provider.

Filiz Toprak Esin
Gün + Partners

Filiz Toprak Esin is a managing associate at Gün + Partners and has been working for the firm since 2006. Her practice is focused on corporate and mergers and acquisitions (M&A), competition and business crimes and anti-corruption.

Filiz has been involved in various M&A deals and has assisted several clients with investments in Turkey. Filiz is providing services to clients on daily transactions, from establishment to liquidation.

Filiz has broad experience in compliance matters, including competition and white-collar crimes. She has assisted various major multinational clients in their fight against corruption and provides preventive advice about their compliance process. At the same time, she represents executives of clients before relevant authorities and courts regarding white-collar crime-related investigations and court actions.

Alexandros Tsagkalidis
Anagnostopoulos

Alexandros Tsagkalidis is a member of the Athens Bar (2009). He received his education at the School of Law, National University of Athens (2007) and completed his postgraduate studies at the same university in criminal law and criminal procedure (LLM, 2011). He is experienced in fraud, bribery, money laundering and asset recovery cases. Alexandros is a member of the legal experts advisory panel of Fair Trials International.

Nicholas Turner
Clifford Chance

Nicholas Turner is a registered foreign lawyer in Clifford Chance's Hong Kong litigation and dispute resolution team, and specialises in financial crimes, including economic sanctions and anti-money laundering advisory in the financial services sector. He is admitted in the State of New York and is a certified anti-money laundering specialist.

Nicholas' experience in North America and Asia includes anti-money laundering and sanctions consent-order remediation for a major US financial institution, anti-money laundering and sanctions risk assessments for a US financial institution, and sanctions advisory for a major US financial institution in Asia. His practice covers new product approval, know-your-customer and product advisory, analysis of wire transfers, customer accounts, investment banking deals, and other transactions under anti-money laundering and sanctions regulations. He offers counsel on investigations, testing and remediation of know-your-customer, sanctions screening and related internal compliance controls, and analysis and advisory in line with US, UN and national sanctions regulations in North America and Asia, and anti-money laundering and sanctions training.

Serrin A Turner
Latham & Watkins

Serrin Turner is a partner in the New York office of Latham & Watkins, where he is a member of the firm's information law, data privacy and cybersecurity practice, white-collar defence and government investigations practice, and complex commercial litigation practice.

A former federal prosecutor and experienced trial lawyer, Mr Turner represents financial institutions and corporations in complex civil litigation, white-collar criminal defence matters, internal corporate investigations, and crisis-management situations, including data breaches and other cybersecurity incidents.

Prior to joining Latham, Mr Turner served for six years as an Assistant US Attorney for the Southern District of New York, where he was the Office's lead cybercrime prosecutor. In that role, Mr Turner handled a wide range of cybercrime investigations and prosecutions, including matters involving computer hacking, data breaches, black-market websites, trafficking in stolen payment card and personal identity information, and money laundering through digital currencies.

Mr Turner's representative experience includes leading the response to a credit card breach experienced by a national retailer, including overseeing the breach investigation. He has also assisted various companies and financial institutions on responding to data breaches and other cybersecurity incidents, including supervising forensic investigations of the incidents.

Heloísa Barroso Uelze
Trench Rossi Watanabe

Heloísa Barroso Uelze joined the firm in 2000 and became a partner in 2005. She is currently the head of the Brazilian public law, government relations and regulatory, and ethics, compliance and investigations practice group. Mrs Uelze has vast experience of working in compliance matters, representing clients both before public administration and the judiciary department. On numerous occasions she has dealt with the federal and state public prosecutors' offices in negotiating deals in matters that involved Brazil's Improbity Law and Clean Companies Act. She has also defended clients' interests before several courts of accounts (at federal, state and municipal levels). Mrs Uelze also works with clients in strengthening their compliance areas, by improving both the internal rules and the mechanisms to enforce those rules. She prepares and reviews internal policies and guidelines, and also provides speeches and training to clients' teams, to make sure everyone is aware of the applicable rules.

Mrs Uelze is recognised as a leading practitioner in such areas of law by various international publications, such as *Chambers*, *LACCA*, *Análise Advocacia* and *PLC*. She graduated at the Pontifical Catholic University of São Paulo Law School and is a specialist in administrative law, constitutional law, tax law and civil procedure.

Thomas Voppichler
Knoetzl

Thomas Voppichler is a counsel at KNOETZL. His practice is focused on business crime matters, asset recovery and international litigation.

An expert in all areas of white-collar crime, Thomas delivers an effective experience to clients through high-profile criminal proceedings, especially in aggressive pursuit of injured parties' recovery of damages suffered through embezzlement, fraud and bribery.

Thomas has extensive experience in conducting internal and external corporate investigations, essential both for revealing internal misconduct and enhancing compliance, and for gathering evidence and preparing for criminal and civil enforcement claims for injured companies.

Thomas also routinely acts as defence counsel in cases involving corporate and business crimes, and handles mission-critical cases for national and international clients. Thomas also maintains significant, active and current expertise in asset tracing and recovery techniques, applied successfully in a wide array of jurisdictions.

With many years of experience in high-profile, complex litigation, Thomas is frequently active as legal counsel to international corporates. In those disputes, mostly concerning the banking, insurance, construction and corporate sectors, clients gain advantage from Thomas's extensive knowledge and experience in proceedings with interim measures, large amounts at stake, and time-sensitive missions.

Donna Wacker
Clifford Chance

Donna Wacker is the head of the Hong Kong contentious regulatory team. She is admitted in Hong Kong, Australia, and England and Wales and has been practising in Asia since 1999.

Donna advises on contentious and advisory regulatory matters in the financial sector, and in complex banking and commercial litigation. She has advised investment banks and brokerages in a wide range of regulatory investigations, including on insider dealing and other forms of market manipulation, global investigations into rate fixing, short selling, algorithmic trading issues, sponsor work for initial public offerings, reporting failures, and a range of system and control issues. Donna is currently advising on a number of litigation matters involving alleged mis-selling of derivatives and other structured products. Donna also leads the firm's contentious insolvency practice and is advising a number of financial institutions in respect of their resolution planning activities.

Donna is ranked as a leading individual in *Chambers* for litigation, contentious regulatory, and restructuring and insolvency work, and is also recognised in *The Legal 500*.

Rebecca Kahan Waldman
Dechert LLP

Rebecca Kahan Waldman is a partner in Dechert's white-collar and securities litigation group. Ms Waldman focuses her practice on complex commercial and securities disputes with an emphasis on litigation involving the banking and financial services sectors, white-collar and internal investigations, and e-discovery. She also has significant trial experience and has served as trial counsel in a number of federal, state and bankruptcy litigations. Ms Waldman is actively involved in recruiting and is also in charge of the New York Office Women's Initiative.

Her significant representations include advising the former chief executive officer of a registered futures commission merchant and broker dealer in civil litigations and congressional and regulatory inquiries arising out of the bankruptcy of a former employer; the former chief risk officer of Fannie Mae against securities fraud charges filed by the SEC in the Southern District of New York; individuals and companies in class action lawsuits alleging violations of federal securities laws; individuals and companies in investigations commenced by the SEC, CFTC, Department of Justice, state attorneys general and Congress; and The Bank of New York Mellon in all aspects of litigation and SEC and CFTC investigations relating to the bankruptcy of Sentinel Management Group.

Ms Waldman was recently named a Rising Star by the *New York Law Journal*. She is also a recipient of the Legal Aid Society's 2018 Pro Bono Publico Award for outstanding service.

Michael Wang
Clifford Chance

Michael Wang is a senior associate in Clifford Chance's litigation and dispute resolution practice. Admitted in Hong Kong in 2012, Michael is a native Mandarin speaker and is fluent in Cantonese.

Michael advises on a broad range of contentious regulatory matters and complex banking and commercial litigation. He regularly advises banks, investment funds, brokerages, asset managers and listed companies in a wide range of regulatory investigations and compliance

issues, including market misconduct, sponsor liability, algorithmic trading and reporting failures. Michael also advises and represents banks and high net worth individuals in a number of high-profile court and tribunal hearings, both local and cross-border, involving mis-selling of structured products and general commercial disputes.

Holly Ware
Slaughter and May

Holly Ware, a partner in Slaughter and May's dispute resolution group, has a broad practice that includes litigation and contentious regulatory and criminal investigations.

She has cross-jurisdictional investigation experience involving both regulatory and prosecuting authorities, including the LIBOR investigations and others relating to bribery and corruption, market abuse, money laundering and data breaches.

Karen Werner
Bofill Mir & Alvarez Jana

Karen Werner is a litigation partner at Chilean law firm Bofill Mir & Alvarez Jana. Mrs Werner studied law at the Catholic University of Chile, where she graduated *magna cum laude*. Ms Werner obtained an LLM from the Columbia Law School in New York (2017), graduating with honours as a Harlan Fiske Stone Scholar.

Mair Williams
Latham & Watkins

Mair Williams' practice focuses on white-collar defence. She has considerable trial experience having started her career as a criminal barrister in chambers, as well as experience in investigations, representing companies and individuals before regulators and prosecuting bodies, and developing compliance policies and practices for international clients.

In addition to her white-collar work, Ms Williams has experience in all manner of complex commercial litigation and has represented clients at every stage from initial pleadings through to trial and appeal.

Ms Williams has conducted a range of internal investigations including an investigation of a financial services firm following a leak of confidential information to the media and an investigation on behalf of a private pension scheme following allegations made by a whistleblower. Her diverse range of representative experience includes representing a director in an investigation by the Financial Reporting Council into discrepancies with annual accounts of a FTSE 250 company and representing a publicly listed investment firm in investigations by the Financial Conduct Authority and Serious Fraud Office.

Ms Williams has an active *pro bono* practice focused on representing individuals in the criminal justice system and providing legal advice to charities and NGOs.

Milton L Williams
Walden Macht & Haran LLP

Milt Williams' practice focuses on white-collar criminal and regulatory matters, employment law, litigation and advisory work representing corporations, and complex commercial litigation. He has litigated discrimination claims, Dodd-Frank and Sarbanes-Oxley retaliation claims, and SEC and IRS whistleblower claims on behalf of employees, and he has tried over 55 cases (both civil and criminal) to verdict. Before joining Walden Macht & Haran, Milt served as Deputy General Counsel and Chief Compliance Officer at Time Inc, where his responsibilities included compliance, the Foreign Corrupt Practices Act, OFAC, and Sarbanes-Oxley, as well as intellectual property, privacy, data security, and other cutting edge areas. At Time Inc, Milt actively litigated a variety of employment law matters on behalf of the company concerning race, age and gender discrimination, and independent contractor litigation. In 2013, Milt was appointed co-chair of the Moreland Commission to investigate public corruption. Earlier in his career, Milt served as an Assistant US Attorney in the US Attorney's Office (USAO) for the SDNY. His last assigned unit in the USAO was the Securities and Commodities Fraud Force. He was also an Assistant District Attorney in the Manhattan District Attorney's Office. Milt is a graduate of Amherst College and the University of Michigan Law School in Ann Arbor.

Nicholas Williams
Freshfields Bruckhaus Deringer

Nick Williams is a partner within Freshfields' dispute resolution practice in London and a member of the corporate crime group. As well as handling a broad range of large-scale, multi-jurisdictional commercial disputes, Nick has advised on a range of internal corporate, regulatory and criminal investigations (including a number of investigations by the SFO) for major corporate clients, including in the professional services, retail and pharmaceuticals sectors.

Alison Wilson
Linklaters LLP

Alison Wilson is a contentious regulatory partner at Linklaters in London. She advises market-leading financial institutions, particularly in the retail bank sector, on their most significant FCA enforcement investigations, as well as on a range of internal investigations. She routinely advises firms on their investigation of whistleblowing concerns, including in an FCA enforcement context. She also has experience advising clients under investigation by the SFO and overseas enforcement agencies. Alison's contentious regulatory experience includes pre-enforcement work, often helping clients through section 166 Financial Services and Markets Act reviews, thematic reviews and FCA executive procedures.

Alison was listed as one of *Global Investigations Review*'s 40 under 40 investigations lawyers in 2017, as well as being included as a Rising Star in Litigation in *Legal Week*'s 2016 list.

Alison's extensive bank sector knowledge has been supplemented by three bank secondments.

Kyle Wombolt
Herbert Smith Freehills

Kyle Wombolt is the global head of Herbert Smith Freehills' corporate crime and investigations practice. He has been described by clients as 'one of the cornerstones of investigations work in Asia' and 'an exceptional lawyer'. Based in Hong Kong, Kyle has 20 years' experience in Asia and has led investigations and compliance projects in more than 40 countries worldwide. He focuses on multi-jurisdictional anti-corruption, regulatory, fraud and accounting investigations, as well as trade and sanctions issues involving multinational and major regional corporates. He has extensive experience in dealing with a broad group of government agencies and regulators in key jurisdictions in Asia, Europe, Australia and the United States.

Kyle also has a diverse range of experience in implementing anti-corruption compliance programmes for a broad range of clients, including investment banks and other financial institutions and multinational companies. He regularly advises clients on corruption risks associated with a wide range of transactions, including initial public offerings, mergers and acquisitions, and joint ventures.

Kyle is admitted to practise in Hong Kong, California and New York, and is a registered foreign lawyer in England and Wales.

William Wong
Clifford Chance

William Wong is a Hong-Kong based consultant in Clifford Chance's litigation and dispute resolution practice. He is admitted in Hong Kong, and England and Wales, and he has more than 10 years of experience in banking litigation, white-collar crime and all aspects of contentious regulatory work, and he regularly advises a broad range of institutional clients (investment banks, private banks, insurance companies, hedge funds and asset managers) and individual clients (senior executives of listed corporations and financial institutions) in local and cross-border regulatory investigations. He also advises on commercial litigation and employment-related matters from time to time.

Before joining Clifford Chance, William had held in-house positions at two bulge-bracket investment banks, advising on their regulatory and compliance issues and internal investigations. With his in-house experience and trilingual capability, William is a popular counsel of choice, particularly when clients require first-class advice and Chinese language support.

He is ranked as a Next Generation Lawyer in Hong Kong for dispute resolution in the 2017 and 2018 editions of *The Legal 500*.

Alistair Wood
Pinsent Masons LLP

Alistair Wood is a solicitor at Pinsent Masons LLP and a member of the international white-collar crime, investigation and compliance team. He specialises in the conduct of investigations, self-reporting and anti-bribery compliance.

Matthew Worby
Jenner & Block London LLP

Matthew Worby is an associate in Jenner & Block's investigations, compliance and defence practice group. Matthew has experience of representing both international corporates in investigations and defending individuals against prosecution by the SFO.

Zaneta Wykowska
Ropes & Gray LLP

Zaneta Wykowska is an associate at Ropes & Gray in London, who frequently advises multinational corporations and individuals involved in government-initiated and internal investigations of cross-border anti-corruption and anti-money laundering matters, in addition to other matters involving alleged fraud.

Wendy Wysong
Clifford Chance

Wendy Wysong leads Clifford Chance's Asia-Pacific anti-corruption and trade controls practice, maintaining offices in Hong Kong and Washington, DC. Her practice focuses on regulatory compliance and white-collar defence under international law, including the Foreign Corrupt Practices Act, International Traffic in Arms Regulations, Export Administration Regulations, Office of Foreign Assets Control economic sanctions and US anti-boycott laws, as well as government fraud and public corruption.

As a former Assistant US Attorney in Washington, DC, and the Deputy Assistant Secretary for Export Enforcement, Bureau of Industry and Security, Department of Commerce, Wendy counsels and defends clients based on her unique combination of experience and insight as both a prosecutor and regulator before courts and agencies.

Wendy is ranked in Band One in *Chambers for Corporate Investigations/Anti-Corruption*, and was named a Global Elite Thought Leader by *Who's Who Legal: Investigation*. She and her team received unprecedented dual recognition in 2017 as the Export Controls Law Firm of the Year, USA and the Export Controls/Sanctions Law Firm of the Year, Rest of the World by *World Export Controls Review*. Wendy led and coordinated the international team that represented a Chinese telecommunications company charged with violating US export controls and sanctions, securing the first-ever temporary general licence enabling the company to stay in business during the multi-agency investigation.

Bruce E Yannett
Debevoise & Plimpton LLP

Bruce Yannett is deputy presiding partner of the firm and chair of the white-collar and regulatory defence practice at Debevoise & Plimpton. He focuses on white-collar criminal defence, regulatory enforcement and internal investigations. He represents a broad range of companies, financial institutions and their executives in matters involving securities fraud, accounting fraud, foreign bribery, cybersecurity, insider trading and money laundering. He has extensive experience representing corporations and individuals outside the United States in responding to inquiries and investigations.

Chambers Global 2018 recognises Mr Yannett as a Band 1 practitioner for FCPA matters, and *Chambers USA* 2018 recognises Mr Yannett as a Band 1 practitioner for both white-collar criminal defence and FCPA matters. Clients praise his work as 'excellent' and describe him as a 'very strong communicator and litigator' and a 'leading light in the field', noting that 'he has real gravitas about him', giving him the 'immediate respect of everybody in the room'. In a similar vein, *The Legal 500: United States* calls him a 'superstar', *Lawdragon* recognises him as one of the 500 leading lawyers in America, and *Benchmark Litigation* names him a 'Litigation Star'. Further, in selecting Debevoise as 'Litigation Department of the Year' in 2014, *The American Lawyer* stated that Mr Yannett's work on the groundbreaking Siemens FCPA internal investigation, which spanned 34 countries, and settlement with US and German authorities, 'cemented his credibility with regulators' on subsequent matters.

He is a member of the American Law Institute. Mr Yannett is on the board of advisers for the New York University programme on corporate compliance and enforcement.

Early in his career, Mr Yannett served in the Office of Independent Counsel: Iran/Contra and as an assistant United States attorney.

Steve Young
Association of Corporate Investigators

Steve Young spent 20 years in UK law enforcement with the City of London and Metropolitan Police services investigating economic crime. He specialises in the proactive investigation of banking fraud, money laundering, bribery and corruption. He worked internationally with multiple law enforcement agencies in the United States, Europe and Asia. This was followed by six years as Citigroup EMEA regional director of investigations, and eight years as Barclays' global head of investigations for investment banking and wealth management. At Barclays, he managed a team of corporate investigators who worked globally on all aspects of internal and external economic crime, whistleblowing investigations, regulatory investigations and litigation support. To date, he has 39 years of international economic crime experience in both law enforcement and corporate environments. He speaks frequently on economic crime investigations at legal, corporate and law enforcement events. Steve is currently head of fraud and investigations at Lombard Odier & Co Ltd, based in Geneva and chief executive officer of the Association of Corporate Investigators.

Jerina Zapanti
Anagnostopoulos

Jerina (Gerasimoula) Zapanti is a member of the Athens Bar (2001) and the Hellenic Criminal Bar Association (2007). She has considerable experience in cross-border cases involving fraud, bribery, cartel offences, tax offences and money laundering. She is very active in internal corporate investigations and risk management assessment for national and multi-national corporations.

María Haydée Zegarra
Rebaza, Alcázar & De Las Casas

María Haydée Zegarra leads the labour and employment law practice and has extensive experience in providing legal counselling on personnel hiring and layoffs, collective bargaining, outsourcing of workforce, implementation of internal policies and internal investigations for companies in the fishing, port industry, telecommunications, financial, insurance, agro-industrial and aeronautical sectors.

She has been highlighted by our clients for the preparation of strong defence strategies in relation to judicial processes and administrative inspections thanks to her knowledge of the client's operational know-how and more than 15 years of experience in the labour field.

María Haydée actively participates in training workshops for companies on labour issues, such as employment modalities, management of overtime working, disciplinary sanctions management, employment of foreign employees, among others.

Julie Zorrilla
Navacelle

Julie Zorrilla worked as a trainee in the Directorate of Legal Affairs at the French Ministry of Economic Affairs and Finance in 2012 and was a law clerk to the Paris Court of Appeal in 2011.

During the past few years, Ms Zorrilla has worked on complex cross-border financial and criminal matters (including embargoes, index manipulation and SSA) involving top executives and large foreign and French lending institutions. Ms Zorrilla has also handled large-scale corruption matters, advising on both legal and communication strategies.

Appendix 2

Contributors' Contact Details

Addleshaw Goddard LLP
Milton Gate
60 Chiswell Street
London, EC1Y 4AG
United Kingdom
Tel: +44 20 7606 8855
nichola.peters@addleshawgoddard.com
michelle.dekluyver@addleshawgoddard.com
www.addleshawgoddard.com

Allen & Overy LLP
1101 New York Avenue, NW
Washington, DC 20005
United States
Tel: +1 202 683 3800
Fax: +1 202 683 3999
anthony.mansfield@allenovery.com

1221 Avenue of the Americas
New York, NY 10020
United States
Tel: +1 212 610 6300
Fax: +1 212 610 6399
eugene.ingoglia@allenovery.com

www.allenovery.com

Anagnostopoulos
Patriarchou Ioakeim 6
106 74 Athens
Greece
Tel: +30 210 729 2010
Fax: +30 210 729 2015
ianagnostopoulos@iag.gr
jzapanti@iag.gr
atsagkalidis@iag.gr
www.iag.gr

Association of Corporate Investigators
Kemp House
152-160 City Road
London, EC1V 2NX
Tel: +44 20 3129 8522
admin@my-aci.com
www.my-aci.com

Baker McKenzie LLP
100 New Bridge Street
London, EC4V 6JA
United Kingdom
Tel: +44 20 7919 1000
Fax: +44 20 7919 1999
joanna.ludlam@bakermckenzie.com

452 Fifth Avenue
New York, NY 10018
United States
Tel: +1 212 626 4337
Fax: +1 212 310 1696
william.devaney@bakermckenzie.com

www.bakermckenzie.com

BCL Solicitors LLP
51 Lincoln's Inn Fields
London, WC2A 3LZ
United Kingdom
Tel: +44 20 7430 2277
Fax: +44 20 7430 1101
rsallybanks@bcl.com
aamin@bcl.com
jflynn@bcl.com
www.bcl.com

BDO USA, LLP
100 Park Avenue
New York, NY 10017
United States
Tel: +1 212 885 8379
gpomerantz@bdo.com
nsliger@bdo.com
mbarba@bdo.com
www.bdo.com

Bofill Mir & Alvarez Jana
Avenida Andrés Bello 2711, 8th Floor
Torre Costanera
Las Condes
Santiago 7550611
Chile
Tel: +56 227 577 600
Fax: +56 227 577 813
ajana@bmaj.cl
kwerner@bmaj.cl
www.bmaj.cl

Borden Ladner Gervais LLP
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Suite 3400
Toronto
Ontario, M5H 4E3
Canada
Tel: +1 416 367 6000
Fax: +1 416 367 6749
ghamilton@blg.com
mbarutciski@blg.com
www.blg.com

Brown Rudnick LLP
8 Clifford Street
London, W1S 2LQ
United Kingdom
Tel: +44 20 7851 6000
Fax: +44 20 7851 6100
aamole@brownrudnick.com
www.brownrudnick.com

Brunswick Group LLP
16 Lincoln's Inn Fields
London, WC2A 3ED
United Kingdom
Tel: +44 20 7404 5959
Fax: +44 20 7831 2823
cpotter@brunswickgroup.com

600 Massachusetts Avenue, NW
Suite 350
Washington, DC 20001
United States
Tel: +1 202 393 7337
Fax: +1 202 898 1588
kbailey@brunswickgroup.com

www.brunswickgroup.com

Cadwalader, Wickersham & Taft LLP
700 Sixth Street, NW
Washington, DC 20001
United States
Tel: +1 202 862 2456
jodi.avergun@cwt.com
anne.tompkins@cwt.com
robert.duncan@cwt.com
www.cadwalader.com

700 Sixth Street, NW
Washington, DC 20001
United States
Tel: +1 202 862 2200
Fax: +1 202 862 2400
joseph.moreno@cwt.com

200 Liberty Street
New York, NY 10281
United States
Tel: +1 212 504 6000
Fax: +1 212 504 6666
todd.blanche@cwt.com

www.cadwalader.com

Clifford Chance
Clifford Chance
Level 7, 190 St George's Terrace
Perth, WA 6000
Australia
Tel: +61 8 9262 5555
Fax: +61 8 9262 5522
ben.luscombe@cliffordchance.com
kirsten.scott@cliffordchance.com
lara.gotti@cliffordchance.com

Level 16, 1 O'Connell Street
Sydney, NSW 2000
Australia
Tel +61 2 8922 8000
Fax +61 2 8922 8088
tim.grave@cliffordchance.com
angela.pearsall@cliffordchance.com

Clifford Chance
27th Floor, Jardine House
One Connaught Place
Hong Kong
Tel: +852 2825 8888
Fax: +852 2825 8800
donna.wacker@cliffordchance.com
wendy.wysong@cliffordchance.com
anita.lam@cliffordchance.com
william.wong@cliffordchance.com
michael.wang@cliffordchance.com
nicholas.turner@cliffordchance.com

Clifford Chance LLP
10 Upper Bank Street
Canary Wharf
London, E14 5JJ
United Kingdom
Tel: +44 20 7006 1000
Fax: +44 20 7006 5555
luke.tolaini@cliffordchance.com

Clifford Chance US LLP
31 West 52nd Street
New York, NY 10019-6131
United States
Tel: +1 212 878 8000
Fax: +1 212 878 8375
christopher.morvillo@cliffordchance.com
daniel.silver@cliffordchance.com
benjamin.berringer@cliffordchance.com
tara.mcgrath@cliffordchance.com
kaitlyn.ferguson@cliffordchance.com

www.cliffordchance.com

Cloth Fair Chambers
39-40 Cloth Fair
London, EC1A 7NT
United Kingdom
Tel: +44 20 7710 6444
nicholas.purnell@clothfairchambers.com
www.clothfairchambers.com

CMS Cameron McKenna Nabarro Olswang LLP SCP
S-Park, 11–15 Tipografilor Street
B3–B4, 4th Floor
District 1
013714 Bucharest
Romania
Tel: +40 21 40 73 800
Fax: +40 21 40 73 900
gabriel.sidere@cms-cmno.com
www.cms.law

Corker Binning
The Cursitor Building
38 Chancery Lane
London, WC2A 1EN
United Kingdom
Tel: +44 20 7353 6000
Fax: +44 20 7353 6008
jp@corkerbinning.com
as@corkerbinning.com
www.corkerbinning.com

Cravath, Swaine & Moore LLP
825 Eighth Avenue
New York, NY 10019
United States
Tel: +1 212 474 1000
Fax: +1 212 474 3700
jburetta@cravath.com
mlew@cravath.com
cgans@cravath.com
aeisen@cravath.com
www.cravath.com

Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
United States
Tel: +1 212 909 6000
Fax: +1 212 909 6836
beyannett@debevoise.com
dsarratt@debevoise.com
www.debevoise.com

Dechert LLP
1095 Avenue of the Americas
New York, NY 10036-6797
United States
Tel: +1 212 698 3500
Fax: +1 212 698 3599
hector.gonzalez@dechert.com
rebecca.waldman@dechert.com

160 Queen Victoria Street
London, EC4V 4QQ
United Kingdom
Tel: +44 20 7184 7000
Fax: +44 20 7184 7001
caroline.black@dechert.com
lisa.foley@dechert.com

www.dechert.com

DLA Piper LLP
1251 Avenue of the Americas
New York, NY 10020-1104
United States
Tel: +1 212 335 4500
Fax: +1 212 335 4501
john.hillebrecht@dlapiper.com
lisa.tenorio@dlapiper.com
eric.christofferson@dlapiper.com
www.dlapiper.com

Fornari e Associati
Via Chiossetto 18
20122 Milan
Italy
Tel: +39 02 541 222 06
e.difiorino@fornarieassociati.com
www.fornarieassociati.com

Fountain Court Chambers
Fountain Court
Temple
London, EC4Y 9DH
United Kingdom
Tel: +44 20 7583 3335
Fax: +44 20 7353 0329
eld@fountaincourt.co.uk
rl@fountaincourt.co.uk
nxl@fountaincourt.co.uk
to@fountaincourt.co.uk
rjl@fountaincourt.co.uk
ser@fountaincourt.co.uk
www.fountaincourt.co.uk

Freshfields Bruckhaus Deringer
65 Fleet Street
London, EC4Y 1HS
United Kingdom
Tel: +44 20 7936 4000
Fax: +44 20 7832 7001
ali.sallaway@freshfields.com
matthew.bruce@freshfields.com
ben.morgan@freshfields.com
nicholas.williams@freshfields.com
www.freshfields.com

Fox Williams LLP
10 Finsbury Square
London, EC2A 1AF
United Kingdom
Tel: +44 20 7628 2000
Fax: +44 20 7628 2100
jcarlton@foxwilliams.com
sganatra@foxwilliams.com
dmurphy@foxwilliams.com
www.foxwilliams.com

Gleiss Lutz
Taunusanlage 11
60329 Frankfurt
Germany
Tel: +49 69 95514 0
Fax: +49 69 95514 198
eike.bicker@gleisslutz.com
christoph.skoupil@gleisslutz.com
marcus.reischl@gleisslutz.com

Lautenschlagerstrasse 21
70173 Stuttgart
Germany
Tel: +49 711 8997 0
Fax: +49 711 8550 96
christian.steinle@gleisslutz.com

www.gleisslutz.com

Goodwin
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
United States
Tel: +1 212 813 8800
Fax: +1 212 355 3333
rstrassberg@goodwinlaw.com
mspillane@goodwinlaw.com
www.goodwinlaw.com

Gün + Partners
Kore Şehitleri Cad. 17
Zincirlikuyu 34394
Istanbul
Turkey
Tel: + 90 212 354 00 00
Fax: + 90 212 274 20 95
filiz.toprak@gun.av.tr
asena.keser@gun.av.tr
www.gun.av.tr

Herbert Smith Freehills
Herbert Smith Freehills LLP
28th Floor Office Tower
Beijing Yintai Centre
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022
China
Tel: +86 10 6535 5000/5133
Fax: +86 10 6535 5055
mark.chu@hsf.com

Herbert Smith Freehills LLP
38th Floor, Bund Centre
222 Yan An Road East
Shanghai 200002
China
Tel: +86 21 2322 2000
Fax: +86 21 2322 2322
tracey.cui@hsf.com

Herbert Smith Freehills
23rd Floor, Gloucester Tower
15 Queen's Road Central
Hong Kong
Tel: +852 2845 6639
Fax: +852 2845 9099
christine.cuthbert@hsf.com
pamela.kiesselbach@hsf.com
kyle.wombolt@hsf.com

Herbert Smith Freehills LLP
Exchange House
Primrose Street
London, EC2A 2EG
United Kingdom
Tel: +44 20 7466 2580
Fax: +44 20 7374 0888
susannah.cogman@hsf.com
www.herbertsmithfreehills.com

Homburger
Prime Tower
Hardstrasse 201
8005 Zurich
Switzerland
Tel: +41 43 222 10 00
Fax: +41 43 222 15 00
flavio.romerio@homburger.ch
claudio.bazzani@homburger.ch
katrin.ivell@homburger.ch
reto.ferrari-visca@homburger.ch
www.homburger.ch

Jenner & Block
Jenner & Block London LLP
Level 17, Tower 42
25 Old Broad Street
London, EC2N 1HQ
United Kingdom
Tel: +44 330 060 5400
Fax: +44 330 060 5499
khagedorn@jenner.com
rdalling@jenner.com
mworby@jenner.com

Jenner & Block LLP
353 N Clark Street
Chicago, IL 60654
United States
Tel: +1 312 222 9350
glittleton@jenner.com
criely@jenner.com
www.jenner.com

Jones Day
250 Vesey Street
New York, NY 10281-1047
United States
Tel: +1 212 326 3808
Fax: +1 212 755 7306
jloonam@jonesday.com
creardon@jonesday.com
www.jonesday.com

Knoetzl
Herrengasse 1
1010 Vienna
Austria
Tel: +43 1 34 34 000 200
Fax: +43 1 34 34 000 999
bettina.knoetzl@knoetzl.com
thomas.voppichler@knoetzl.com
www.knoetzl.com

Kingsley Napley LLP
Knights Quarter
14 St John's Lane
London, EC1M 4AJ
United Kingdom
Tel: +44 20 7814 1200
Fax: +44 20 7490 2288
cday@kingsleynapley.co.uk
lhodges@kingsleynapley.co.uk
www.kingsleynapley.co.uk

Latham & Watkins
99 Bishopsgate
London, EC2M 3XF
United Kingdom
Tel: +44 20 7710 3001
stuart.alford.qc@lw.com
gail.crawford@lw.com
hayley.pizzey@lw.com
mair.williams@lw.com

885 Third Avenue
New York, NY 10022-4834
United States
Tel: +1 212 906 1330
serrin.turner@lw.com

505 Montgomery Street
Suite 2000
San Francisco, CA 94111-6538
United States
Tel: +1 415 395 8040
max.mazzelli@lw.com

www.lw.com

Law Offices of Panag and Babu
No. 82, First Floor
Phase III, Okhla Industrial Estate
New Delhi, 110020
India
Tel: +91 011 49996 800
sherbir@pblawoffices.com
tanya.ganguli@pblawoffices.com
lavanyaa.chopra@pblawoffices.com
www.pblawoffices.com

Linklaters LLP
One Silk Street
London, EC2Y 8HQ
United Kingdom
Tel: +44 20 7456 2000
Fax: +44 20 7456 2222
jillian.naylor@linklaters.com
alison.wilson@linklaters.com
sinead.casey@linklaters.com
elly.proudlock@linklaters.com
www.linklaters.com

Marval O'Farrell & Mairal
Avenida Leandro N. Alem 882
(C1001AAQ) Buenos Aires
Argentina
Tel: +54 11 4310 0100
Fax: +54 11 4310 0200
pse@marval.com
glo@marval.com
mls@marval.com
www.marval.com

Matheson
70 Sir John Rogerson's Quay
Dublin 2
Ireland
Tel: +353 1 232 2000
Fax: +353 1 232 3333
claire.mcloughlin@matheson.com
karen.reynolds@matheson.com
ciara.dunny@matheson.com
www.matheson.com

Matrix Chambers
Griffin Building
Gray's Inn
London, WC1R 5LN
United Kingdom
Tel: +44 20 7404 3447
Fax: +44 20 7404 3448
edwardcraven@matrixlaw.co.uk
alexbailin@matrixlaw.co.uk
www.matrixlaw.co.uk

Miller & Chevalier Chartered
900 16th Street NW
Washington, DC 20006
United States
Tel: +1 202 626 5800
Fax: +1 202 626 5801
totoole@milchev.com
wbarry@milchev.com
mlaporte@milchev.com
www.millerchevalier.com

Navacelle
60 rue Saint-Lazare
75009 Paris
France
Tel: +33 1 48 78 76 78
Fax: +33 9 81 70 49 00
sdenavacelle@navacellelaw.com
sdossantos@navacellelaw.com
jzorrilla@navacellelaw.com
cduverne@navacellelaw.com
www.navacellelaw.com

Nokia Corporation
3 Sheldon Square
Paddington
London, W2 6PY
United Kingdom
femi.thomas@nokia.com
Tel: +44 7785 399 642
tapan.debnath@nokia.com
Tel: +44 7342 089 528
www.nokia.com

Outer Temple Chambers
222 Strand
London, WC2R 1BA
United Kingdom
Tel: +44 20 7353 6381
Fax: +44 870 220 3256
michael.bowesqc@outertemple.com
www.outertemple.com

Philippi Prietocarrizosa Ferrero DU & Uría – PPU
Carrera 9 #74-08
Office 105
Bogotá
Colombia
Tel: +571 3268600
Fax: +571 3268610
pamela.alarcon@ppulegal.com
diego.cardona@ppulegal.com
www.ppulegal.com

Pinsent Masons LLP
30 Crown Place
Earl Street
London, EC2A 4ES
United Kingdom
Tel: +44 20 7418 7000
Fax: +44 20 7418 7050
tom.stocker@pinsentmasons.com
neil.mcinnes@pinsentmasons.com
laura.gillespie@pinsentmasons.com
stacy.keen@pinsentmasons.com
olga.tocewicz@pinsentmasons.com
alistair.wood@pinsentmasons.com
rebecca.devaney@pinsentmasons.com
www.pinsentmasons.com

Rajah & Tann Singapore LLP
9 Straits View
Marina One West Tower, #06-07
Singapore 018937
Tel: +65 6232 0260/0590
danny.ong@rajahtann.com
sheila.ng@rajahtann.com
https://sg.rajahtannasia.com

Rebaza, Alcázar & De Las Casas
Av. Víctor Andrés Belaúnde 147
Vía Principal 133, Pisos 2 y 3
Edificio Real Dos
San Isidro
Lima 27
Peru
Tel: +511 442 5100
Fax: +511 442 5100
alberto.rebaza@rebaza-alcazar.com
augusto.loli@rebaza-alcazar.com
hector.gadea@rebaza-alcazar.com
mariahaydee.zegarra@rebaza-alcazar.com
sergio.mattos@rebaza-alcazar.com
www.rebaza-alcazar.com

Reed Smith LLP
1901 Avenue of the Stars
Suite 700
Los Angeles, CA 90067-6078
United States
Tel: +1 310 734 5200
Fax: +1 310 734 5299
fmok@reedsmith.com

10 South Wacker Drive
40th Floor
Chicago, IL 60606-7507
United States
Tel: +1 312 207 1000
Fax: +1 312 207 6400
esussman@reedsmith.com
bbolerjack@reedsmith.com

599 Lexington Avenue
22nd Floor
New York, NY 10022
United States
Tel: +1 212 521 5400
Fax: +1 212 521 5450
jachilles@reedsmith.com

www.reedsmith.com

Ropes & Gray LLP

60 Ludgate Hill
London, EC4M 7AW
United Kingdom
Tel: +44 20 3201 1500
Fax: +44 20 3201 1501
judith.seddon@ropesgray.com
amanda.raad@ropesgray.com
sean.seelinger@ropesgray.com
sarah.lambert-porter@ropesgray.com
chris.stott@ropesgray.com
matthew.burn@ropesgray.com
zaneta.wykowska@ropesgray.com

Prudential Tower
800 Boylston Street
Boston, MA 02199
United States
Tel: +1 617 951 7000
Fax: +1 617 951 7050
sara.berinhout@ropesgray.com

32nd Floor
191 North Wacker Drive
Chicago, IL 60606
United States
Tel: +1 312 845 1200
Fax: +1 312 845 5500
jaime.feeney@ropesgray.com

1211 Avenue of the Americas
New York, NY 10036
United States
Tel: +1 212 596 9600
Fax: +1 212 596 9090
michael.mcgovern@ropesgray.com
meghan.gilliganpalermo@ropesgray.com

2099 Pennsylvania Avenue, NW
Washington, DC 20006-6807
United States
Tel: +1 202 508 4655
Fax: +1 202 508 4650
ama.adams@ropesgray.com

www.ropesgray.com

Russell McVeagh

Level 30, Vero Centre
48 Shortland Street
Auckland 1140
New Zealand
Tel: +64 9 367 8000
Fax +64 9 367 8163
polly.pope@russellmcveagh.com
kylie.dunn@russellmcveagh.com

Level 24, Dimension Data House
157 Lambton Quay
Wellington 6143
New Zealand
Tel: +64 4 499 9555
Fax: +64 4 499 9556
emmeline.rushbrook@russellmcveagh.com

www.russellmcveagh.com

Skadden, Arps, Slate, Meagher & Flom (UK) LLP
40 Bank Street
Canary Wharf
London, E14 5DS
United Kingdom
Tel: +44 20 7519 7000
Fax: +44 20 7519 7070
elizabeth.robertson@skadden.com
www.skadden.com

Slaughter and May
One Bunhill Row
London, EC1Y 8YY
United Kingdom
Tel: +44 20 7600 1200
Fax: +44 20 7090 5000
jonathan.cotton@slaughterandmay.com
holly.ware@slaughterandmay.com
www.slaughterandmay.com

Sofunde Osakwe Ogundipe & Belgore
7th Floor
St Nicholas House
26 Catholic Mission Street
Lafiaji Lagos
Nigeria
Tel: +234 1 462 2502/ 897 2065
Fax: +234 1 462 2501
boogundipe@sooblaw.com
oaogundipe@sooblaw.com
www.sooblaw.com

Sullivan & Cromwell LLP
125 Broad Street
New York, NY 10004-2498
United States
Tel: +1 212 558 4000
Fax: +1 212 558 3588
bourtinn@sullcrom.com
www.sullcrom.com

Trench Rossi Watanabe
Rua Lauro Muller, No. 116, Conj. 2802
Edifício Rio Sul Center
Rio de Janeiro 22290-906
Brazil
Tel: +55 21 2206 4929/4900
felipe.ferenzini@trenchrossi.com

Rua Arq. Olavo Redig de Campos, 105
31º andar
Edifício EZ Towers, Torre A
São Paulo 04711-904
Brazil
Tel: +55 11 3048 6800/5506 3455
heloisa.uelze@trenchrossi.com
joao.gameiro@trenchrossi.com

www.trenchrossi.com

Von Wobeser y Sierra, SC
Paseo de los Tamarindos 60, 4th Floor
Bosques de las Lomas
Cuajimalpa de Morelos
05120 Mexico City
Mexico
Tel: +52 55 5258 1039
Fax: +52 55 5258 1099
dsierra@vwys.com.mx

www.vonwobeserysierra.com

Walden Macht & Haran LLP
One Battery Park Plaza, 34th Floor
New York, NY 10004
United States
Tel: +1 212 335 2030
Fax: +1 212 335 2040
mwilliams@wmhlaw.com
apatel@wmhlaw.com
jgardener@wmhlaw.com
www.wmhlaw.com

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-228-2