GIR INSIGHT

ASIA-PACIFIC INVESTIGATIONS REVIEW 2020

ASIA-PACIFIC
INVESTIGATIONS REVIEW 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2019
For further information please contact Natalie.Clarke@lbresearch.com

LAW BUSINESS RESEARCH

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

www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

ISBN: 978-1-83862-225-1

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Cross-border overviews

Country chapters

Preface

Welcome to the *Asia-Pacific Investigations Review 2020*, a *Global Investigations Review* special report. *Global Investigations Review* is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing, telling them all they need to know about everything that matters.

Throughout the year, the *GIR* editorial team delivers daily news, surveys and features; organises the liveliest events ('GIR Live'); and provides our readers with innovative tools and know-how products. In addition, assisted by external contributors, we curate a range of comprehensive regional reviews – online and in print – that go deeper into developments than our journalistic output is able.

The *Asia-Pacific Investigations Review 2020*, which you are reading, is part of that series. It contains insight and thought leadership from 37 pre-eminent practitioners from the region. Across 16 chapters, spanning around 200 pages, it provides an invaluable retrospective and primer. All contributors are vetted for their standing and knowledge before being invited to take part.

Together, these contributors capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic. This edition covers Australia, Cambodia, China, Hong Kong, India, Indonesia, Laos, Myanmar, Singapore, Thailand and Vietnam in jurisdictional overviews. It also looks at the impact of AI, data privacy, forensic accounting and law enforcement in multi-jurisdictional investigations.

If you have any suggestions for future editions, or want to take part in this annual project, we would love to hear from you.

Please write to insight@globalinvestigationsreview.com.

Global Investigations Review
London
August 2019

China: A New Normal Amid Rising Trade Tensions

Dora W Wang, Michael Lowell, Peter Witherington and Jessica Tian
Reed Smith

Introduction

Investigations in China have been undergoing a transformation in recent years as the rapidly changing commercial and legal environment in China and around the world have created a set of new regulatory and compliance challenges for multinational companies. As the Chinese economy and the ways that companies conduct business in China continue to evolve at a blazing pace, the Chinese legal system has also evolved as the Chinese government has promulgated a host of new laws and regulations.

Responding to these new legal and regulatory changes takes on increased urgency and importance for businesses in China due to the volatility of the political and economic relationship between China and the United States. While recent legal developments are not always explicitly connected to the ongoing trade dispute, the tense environment has influenced the release of new laws, regulations or law enforcement initiatives and strategies in both countries. The effect of these developments on the practice of investigations in China has been significant and is unlikely to fade even after the current trade tensions subside. Instead, companies are now operating in a 'new normal' in the context of investigations in China and will need to confront new types of compliance challenges while complying with stricter and more complex rules governing how to respond to, and how to conduct, investigations. This article outlines this trend by summarising some recent legal developments both in China and the United States, and their impact on various aspects of investigations in China, as well as practical takeaways to help businesses adapt effectively to this 'new normal'.

Trade tensions drive increased scrutiny

As trade tensions between the US and China simmer on with no relief in sight, both governments have intensified enforcement efforts across a broad range of compliance areas, including anti-bribery and anti-corruption (ABAC), antitrust and competition law, cybersecurity and data protection, import and export controls, economic sanctions and other regulatory compliance areas in a number of industries, including life sciences, telecommunications, banking and technology. While some of these developments represent expected reforms by the Chinese

government in support of its efforts to strengthen the rule of law in its fast-evolving domestic market, others appear to be efforts by both the US and Chinese governments to increase regulatory scrutiny across the board in an attempt to gain leverage in ongoing trade negotiations. This has had a particularly sharp effect within China, where both domestic and foreign businesses are now subject to greater scrutiny from both Chinese and US regulators.

On 1 November 2018, the Department of Justice (DOJ) launched its 'China Initiative', a set of policies aimed at fulfilling the DOJ's 'strategic priority of countering Chinese national security threats' and reinforcing '[President Trump's] overall national security strategy', which explicitly states the DOJ's intention to 'identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses'.[1] This development comes as the US Department of Commerce's (DOC) Bureau of Industry and Security (BIS) has placed more Chinese companies on its 'Entity List' – which has the effect of prohibiting the export of most goods, technology and software of US origin or containing US components to listed entities – including a number of prominent Chinese entities doing significant commercial business in the United States.[2] In addition, while changes to the Entity List are publicly released, unpublished export licensing policies administered by BIS prohibit trade in certain export-controlled goods, technology and software to other prominent Chinese entities, including major universities and research centres, which can have unanticipated and detrimental impacts on both these Chinese entities and their US suppliers and partners. Against this backdrop, the compliance risks for trade between the United States and China have never been higher. With aggressive US government enforcement actions against prominent Chinese technology companies capturing the world's attention, such as the record fines levied against ZTE Corporation and the ongoing high-profile case against Huawei, multinational companies (MNCs) with operations in China or who do business with Chinese companies are under pressure to take swift action of their own to conduct pre-emptive internal investigations and to strategise ways to mitigate compliance risks.

The case of Huawei is particularly illustrative. BIS has added Huawei Technologies Co, Ltd and 68 of its non-US affiliates across 26 countries to the Entity List. The DOC has expressed concerns that Huawei 'is engaged in activities that are contrary to US national security or foreign policy interests'.[3] Inclusion on the list effectively prevents Huawei, one of China's most prominent international companies, from doing business with the US, forcing it to procure critical parts and components from non-US sources or to develop them domestically. On 20 May 2019, amid high-level negotiations between the US and Chinese governments, BIS issued Huawei a temporary general licence (TGL), temporarily authorising the sale of certain components to the company and its affiliates within four narrow categories, effective from 19 August 2019.[4] Nonetheless, the TGL does not relieve Huawei and its affiliates of most of the licensing requirements, and it remains unclear whether BIS will place further limits on Huawei after the TGL expires. On 9 July 2019, US Commerce Secretary Wilbur Ross stated in a speech that Huawei

1 US Dept. of Justice, 'Attorney General Jeff Session's China Initiative Fact Sheet' (1 Nov. 2018).

2 15 C.F.R. Part 744, Supplement No. 4.

3 US Bureau of Industry and Security, Addition of Certain Entities to the Entity List (final rule) (16 May 2019).

4 US Bureau of Industry and Security, Temporary General License (final rule) (20 May 2019).

will remain on the Entity List, but stated that BIS may grant licences in specific instances where the proposed exports do not threaten US national security. Of course, the threat to US national security has never been clearly defined so the practical impact of this licensing policy is not yet known.

In the wake of these high-profile actions by US regulators, the Chinese government has also implemented new regulatory measures of its own. On 31 May 2019, the Ministry of Commerce of China (MOFCOM) announced that it will introduce its own black list regime, the Unreliable Entity List. According to official sources, entities or individuals that cause severe damage to Chinese companies through boycotts or other efforts to deny them products or materials for non-commercial reasons are eligible to be added to the list.[5] A draft of the list itself, and the specific measures applicable to the listed entities, will reportedly be released in the near future. Though the exact consequences of inclusion are still unclear, it is likely that listed companies will face significant obstacles in their business operations in China, including in terms of both sales and investment. Observers caught a glimpse of what may be coming on 1 June 2019, when China launched an investigation against FedEx for 'diverting' the delivery of four packages en route to Huawei.[6]

New legal and regulatory challenges across jurisdictions

The investigations of Huawei and FedEx, irrespective of the motivations behind them, have put both domestic Chinese companies and MNCs operating in China on notice. Faced with the prospect of being caught up in the turbulent negotiations between the two governments, many MNCs are choosing to proactively conduct risk assessments or internal investigations to identify potential vulnerabilities and develop mitigation strategies. In some cases, MNCs that may already be exposed are considering whether they may be eligible for prosecutorial leniency through voluntary self-reporting, which is available in the context of certain anti-corruption, antitrust or export controls violations. However, in conducting their own internal investigations, as well as in preparing policies and protocols for responding to government investigations, businesses operating in China should be aware of the latest legal developments and the particular obstacles, hurdles or opportunities they present.

Increased importance of having an effective compliance programme as a defence in government investigations

The voluntary self-reporting of compliance incidents to the DOJ for the purpose of obtaining prosecutorial leniency requires that an entity disclose the misconduct 'prior to an imminent threat of disclosure or government investigation' and 'within a reasonably prompt time after

5 Ministry of Commerce of the People's Republic of China, 'The Spokesman for the Ministry of Commerce Answered Questions about China's Establishment of "Unreliable Entity List' Regime"', (31 May 2019), available at www.mofcom.gov.cn/xwfbh/20190531.shtml (in Chinese).

6 China launches inquiry into FedEx parcel delivery errors: Xinhua. *Reuters*. 14 June 2019, https://www.reuters.com/article/us-huawei-tech-fedex-china-probe/china-launches-inquiry-into-fedex-parcel-delivery-errors-xinhua-idUSKCN1TF17C.

becoming aware of the offense'. Under a 2017 revision to its FCPA Corporate Enforcement Policy, the DOJ will grant a 'presumption of declination' of prosecution to any company that 'voluntarily self-discloses, fully cooperates and timely and appropriately remediates' any violation of the FCPA, provided that there are no aggravating circumstances.[7] Under applicable DOJ policy last updated in 2018, a company must identify all individuals who are 'substantially involved in or responsible for the misconduct at issue' and provide all 'relevant facts' related to their misconduct in order to receive consideration for cooperation credit.[8] In order to meet this requirement, companies need to implement a comprehensive compliance programme that includes mechanisms to detect misconduct and to conduct efficient and effective internal investigations.

While the adequacy and robustness of compliance programmes have long been factors weighed by US prosecutors in white-collar investigations, the existence of a compliance programme or lack thereof has not traditionally been a decisive factor in determining culpability or leniency under analogous Chinese criminal statutes. In recent years, however, not only have the number and complexity of corporate investigations in China increased, the importance of compliance has garnered more and more attention from companies in China due to several recent legislative and policy developments.

Notably, article 7 of the Amended Anti-Unfair Competition Law (AUCL), which came into effect in 2018, provides that 'acts of bribery committed by a staff member of a business operator shall be deemed the conduct of the business operator, unless the business operator has evidence to prove that such acts of the staff member are unrelated to seeking business opportunities or competitive advantage for the business operator'. The AUCL places the onus of compliance on businesses operating in China to present persuasive evidence to show that it should not be held vicariously liable for an employee's misconduct. Accordingly, a company must prove that it has effective compliance controls and that the violation was not carried out in furtherance of the company's interests; and this requires a showing that the company neither endorsed nor acquiesced to the bribery scheme. To meet this new evidentiary burden, companies must carry out more frequent, more timely, and more effective internal investigations.

This development signals a paradigm shift in Chinese white-collar crime jurisprudence, and the effects are already apparent, as several well-known Chinese technology companies, including Meituan, DJI and 360,[9] have voluntarily reported their own executives to the Ministry of Public Security under bribery allegations and the executives involved have been detained and placed under criminal investigation. This shift presents both opportunities and challenges to businesses operating in China, as an effective compliance programme, utilised in combination

7 US Department of Justice, Justice Manual, 9-47.120 - FCPA Corporate Enforcement Policy (2017).

8 US Department of Justice, Justice Manual, 9-28.700 - The Value of Cooperation, Section A (Nov. 2018).

9 Meituan Issues Anticorruption Announcement: Food Delivery Director Sacked, 89 Employees Criminally Investigated, available at https://m.jiemian.com/article/2675706.html?spm=smpc.content.content.1.1550361600023WRl5Apr; DJI Anticorruption Case: Employee who Accepted RMB 25,000 Bribe Sentenced to Three Months Detention, available at https://tech.sina.com.cn/i/2019-07-17/doc-ihytcitm2585529.shtml; Direct Hit: Qihoo 360 Executive Arrested for Bribery; Zhou Hongyi: 'Cut away the rot', available at http://finance.sina.com.cn/fawen/yx/2019-01-30/doc-ihqfskcp1772466.shtml.

with voluntary, truthful and timely self-reporting to the authorities, offers companies a statutorily-provided defence against vicarious liability for the misconduct of their employees that was not previously available. By the same token, however, companies must now invest greater effort and resources in designing, building and maintaining a robust compliance programme and conducting effective investigations.

New rules concerning preservation of data on WeChat and social media applications

In recent years, the universal adoption of social media has dramatically transformed the way employees conduct business around the world and this change can perhaps be felt more strongly in China than anywhere else. In Chinese companies today, vast amounts of sensitive information are communicated using the popular messaging app, WeChat, rather than email. Because such information is frequently subject to discovery in government investigations, the legal systems of both China and the US have begun to grapple with this development.

On 8 March 2019, the DOJ announced revisions to the FCPA Corporate Enforcement Policy (the 2019 FCPA Policy) requiring companies to implement 'appropriate guidance and controls' over communications on ephemeral messaging platforms such as WeChat, in order to ensure the appropriate retention of business records. This reform clearly indicates that the DOJ views the messaging history and chat records of employees to be within the scope of its investigatory authority and that the failure of companies to properly retain records of these conversations could be held against them in a government investigation. Given the ubiquitous use of WeChat for both private and business communications in China, this greatly expands the body of potential evidence that must be collected and reviewed in almost any US government investigation of a Chinese company or of the Chinese operations of an MNC.

While China has yet to release a similar law or regulation mandating the preservation of WeChat or other social media records, the Chinese legal system also places far fewer constraints on prosecutorial authorities' rights to obtain information of all kinds. Therefore, businesses operating in China should assume that these records are subject to review by the Chinese government in any investigation, as an example from 2018 demonstrates, wherein the government was able to restore a WeChat log deleted from a device seized in a government investigation using forensic technology.[10]

Navigating conflicts of law

In some areas, fast-paced legal developments in China and the US have placed businesses in a dilemma: in order to comply with the legal requirements of a foreign jurisdiction such as the US, businesses could be forced to violate domestic Chinese laws. In October 2018, China enacted the International Criminal Justice Assistance Law (ICJAL), which requires companies or individuals in China to seek government approval before providing evidence or information

10 Weixin Responds to Disciplinary Committee's Statement on Recovery of Deleted Mobile Phone Chat Records: 'Records Were Recovered from User's Phone', available at http://www.guancha.cn/industry-science/2018_04_29_455293.shtml.

to foreign prosecutors in support of criminal proceedings in overseas jurisdictions. While it remains to be seen how the new law will be enforced, it inevitably will lead to situations in which companies must choose whether to disregard Chinese law and cooperate with foreign prosecutors or to abide by Chinese law and risk the consequences of being held in contempt or, worse, held liable for obstruction of justice by the US or another foreign government. In one prominent 2019 case, three Chinese banks were held in contempt by a US court after each refused to provide evidence in connection with a money laundering case allegedly involving a Hong Kong front company and a state-owned North Korean bank.[11] Although the banks cited Chinese banking customer privacy laws as justification for the refusal and did not specifically invoke the ICJAL, the law was undoubtedly a factor in their analysis. In its decision, the court noted that the typical process by which such documents would be requested, a formal procedure established by the Mutual Legal Assistance Agreement between the two countries, was unlikely to be successful, as past requests had been routinely stymied by the Chinese government. The court found that, although it was undisputed that the decision would expose the banks to legal penalties under Chinese law, the narrowness of the US government's request and the unique importance of the evidence at issue meant that the US government's significant national security interest in obtaining the documents outweighed the Chinese government's interest in enforcing the relevant Chinese laws. On 31 July 2019, the US Court of Appeals for the District of Columbia upheld the lower court's ruling.[12]

Conflicting interpretations of Chinese law across different jurisdictions can also be a source of uncertainty. In one 2018 example, a group of Chinese manufacturers of vitamin C supplements were sued in an antitrust class action for price-fixing. In their defence, the Chinese companies asserted that their actions were required 'pursuant to Chinese regulations regarding vitamin C export pricing and were, in essence, required by the Chinese government, specifically [the Ministry of Commerce of the People's Republic of China (MOFCOM)], to coordinate prices and create a supply shortage'.[13] In litigation before the US Supreme Court, the Chinese litigants' position was supported by an amicus brief submitted by MOFCOM itself. Nonetheless, the US Supreme Court ruled that it was 'not bound to accord conclusive effect' to a foreign government's interpretation of that government's laws, on its way to a ruling that remanded the case for further proceedings.[14] In the US, the case placed the issue of international comity – that is, whether US courts should defer to the position of a foreign sovereign government on questions of interpretation of its own law – in the spotlight, but for businesses operating in China, it highlights the difficult question of whether abiding by Chinese laws and regulations might trigger legal liability in another country.

11 Hsu, Spencer S, Chinese bank involved in probe on North Korean sanctions and money laundering faces financial 'death penalty,' *Washington Post*, 24 June 2019.

12 *In Re: Sealed Case*, No. 19-5068 (DC Cir. Reissued 6 Aug. 2019).

13 *Animal Sci. Prods., Inc. v Hebei Welcome Pharm. Co. (In re Vitamin C Antitrust Litig.)*, 837 F.3d 175, 180 (2d Cir. 2016).

14 *Animal Science Products, Inc. v Hebei Welcome Pharmaceutical Co. Ltd.*, 585 US ____ (2018).

New restrictions on cross-border data transfer

Beyond specific restrictions on producing evidence for foreign prosecutors, in recent years the Chinese government has also developed a complex regulatory regime governing cross-border data transfers generally. These new laws create additional hurdles for investigations in China, which frequently involve the review of vast amounts of data, often by reviewers who are located outside the country. Even the access of certain data stored in China from a computer terminal located outside the country can constitute a cross-border transfer, and can trigger liability under Chinese law.

Several Chinese laws expressly prohibit the transfer of certain types of data outside of China. The State Secrets Law, for example, has long prohibited the transfer of state secrets outside China and violators are subject to strict criminal penalties. What constitutes 'state secrets' is not always clear cut, but the concept is generally defined to include any data or information that is related to China's 'economic and social development', information related to science and technology or any information that, if released, could pose a threat to Chinese national security.[15] In cases in which a data transfer must be made and it is unclear whether the transfer would trigger liability under the State Secrets Law, a company may need to submit the information to the Chinese government for prior approval. In a more recent development, pre-approvals may also be required under the ICJAL for transmissions of data or information to foreign criminal enforcement authorities, even when the transfer itself is not otherwise specifically prohibited. While the specific procedures required to obtain such pre-approvals have not yet been clearly defined, it will inevitably make the sharing of relevant facts identified in an investigation more complicated and cumbersome.

However, by far the most important recent development in this area came with the promulgation of China's 2017 Cybersecurity Law (CSL), which mandates that 'network operators' – which, in effect, include nearly all businesses – must implement network security measures to protect personal information and important data.[16] Moreover, those operating 'critical information infrastructure' must also ensure that all personal information and important data collated or generated in China is stored on a server that is physically located in China and any cross-border transfer of data is subject to the heightened requirement of security self-assessment and regulatory assessment.[17]

Further building upon the general data transfer provisions in the CSL, China is in the process of developing additional implementation rules to regulate the cross-border transmission of personal information and other sensitive data, which include the draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data (Measures)

15 Law of the People's Republic of China on Guarding State Secrets, Chapter II, article 9 (1 October 2010).

16 'Important data' is defined by the Guidelines as 'data collected by relevant organizations, institutions and individuals that does not involve state secrets but is closely related to national security, economic development and public interest.' See Guidelines for Data Cross-Border Transfer Security Assessment (Draft) (25 Aug. 2017).

17 Cybersecurity Law of the People's Republic of China, article 2 (1 June 2017).

and draft Guidelines for Data Cross-Border Transfer Security Assessment (Guidelines).[18] The Measures list factors that should be weighed when conducting a security assessment of a cross-border transfer of data or information, such as the necessity of the data transfer, the consent of the data subject or owner of the information, the scope and sensitivity of the data itself, the data protection capabilities of the receiving country, the risk of data security breach and the risk of damage to the state and its citizens, among other factors. The Guidelines provide more detailed definitions and instructions regarding cross-border transfer, including examples of scenarios that may qualify as a cross-border data transfer. Some of these are quite broad, such as the transfer of personal information and important data to entities physically located in China but not registered in China or not subject to China's jurisdiction, data that is not transferred outside China but that can be viewed by oversea entities or individuals, or the internal transfer of personal information or important data by a network operator from its offices in China to offices in other countries.

Finally, aside from government regulation, businesses in China must also be aware of the risk of individual litigation. Employees have brought lawsuits or threatened litigation in Chinese courts when data containing their personal information is transferred outside of China, particularly if the data is relied upon in making a finding against them in an internal investigation – for example, from a company's subsidiary in China to its parent company based in the US – if the manner of the transfer does not comply with China's increasingly stringent data privacy laws.

All of these issues represent areas of potential risk, both for MNCs with operations in China and for Chinese companies, including, but not limited to, Chinese-headquartered MNCs that may have reason to transfer data abroad. Consider, for example, an internal investigation conducted by a MNC, that has in-house counsel or compliance personnel who are based in various countries and working in collaboration on the investigation. While the successful handling of the investigation turns on the timeliness of the collection and the sharing of all relevant facts among members of the investigation team, the investigation plan needs to take into consideration that there are specific Chinese laws protecting the privacy rights of individuals as well as important data and state secrets, which may require the data to be localised and reviewed in China. Accordingly, before engaging in any cross-border transfer of personal information or important data, companies in China should consider engaging counsel who is able to make a multi-jurisdictional assessment of the proposed data transfer so as to ensure that the data in question can be transferred lawfully and that all procedural requirements are satisfied. If a transfer poses a significant collateral risk, it is necessary to conduct the review of the data in-country first and adopt procedural safeguards to ensure that subsequent sharing or disclosing of related information does not trigger legal exposure under PRC data protection laws.

18 Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft) (11 Apr. 2017); Guidelines for Data Cross-Border Transfer Security Assessment (Draft) (25 Aug. 2017).

Conclusion

The ability to anticipate an investigation and to expeditiously respond to government inquiries is critical in the present Chinese environment. Without an effective investigation protocol already in place as part of a compliance programme, companies will find it difficult to react to fast-moving developments once an investigation begins. Moreover, many costly enforcement actions can be mitigated or avoided altogether by the quick detection of threats and, if appropriate, a timely self-disclosure to the authorities.

A company with operations in China may choose to involve its local team to conduct such an investigation. However, increasingly, investigations in China are no longer confined to China's territorial borders, with many domestic Chinese businesses and foreign MNCs subject to the jurisdiction of US law, Chinese law and the laws of other nations. As workforces become increasingly mobile and globalised, investigations often entail fact-finding across multiple jurisdictions. Additionally, due to the remarkable growth and globalisation of the Chinese economy, even a Chinese government-launched investigation of a Chinese MNC may have myriad international implications, as these MNCs often have global operations and must therefore comply with multi-jurisdictional laws and regulations that are sometimes in conflict with Chinese law.

In any of these circumstances, it is critical to seek legal advice from an experienced legal team with multi-jurisdictional expertise that can quickly manage the investigation on the ground and navigate diverse legal and business environments in China and outside of China. From the outset of an investigation, the legal team will need to ascertain the locations of the potential evidence and witnesses, obtain the requisite informed consent from data subjects whose personal information will be collected and used in the investigation, review the parameters of the investigatory steps that the company may take based on company policies and pursuant to applicable laws, and manage the flow of data, including but not limited to deciding which data cannot be lawfully transferred outside of China's borders and must instead be reviewed in-country. Further, the legal team will need to quickly determine what evidence must be produced to regulators in a US government-led investigation, including difficult-to-obtain data such as WeChat conversation logs, the collection, use, retention and transfer of which are subject to strict privacy laws in China.

In a government investigation, the company and its legal advisers will also need to balance competing and potentially conflicting obligations imposed by the US and Chinese governments and formulate effective and practical investigation protocols that will allow the company to meet the various evidentiary burdens under both US and Chinese law to minimise corporate liability, and also to make an informed decision on when and how to make a self-disclosure of unlawful conduct in each jurisdiction to receive cooperation credits or leniency. Thus, in the current Chinese compliance environment, whether conducting internal investigations or responding to a government enforcement action conducted by the US or Chinese authorities, businesses must ensure they have access to speedy, comprehensive and coordinated investigatory resources in order to address the complex, cross-border legal questions that will inevitably arise.

Dora W Wang
Reed Smith

Dora is a partner in Reed Smith's global regulatory enforcement group in China and New York. She advises multinational corporations in a broad range of industries on complex cross-border regulatory and compliance matters, internal and government investigations, litigation and dispute resolution matters.

With more than 15 years of experience in government, litigation and client advocacy, Dora's practice combines an in-depth knowledge of the law with a keen understanding of the latest enforcement trends and business conditions in the Greater China region to provide practical and effective legal and strategic counselling to clients.

Dora focuses her practice on multi-jurisdictional investigations of white-collar crimes, employee misconduct, theft of trade secrets, fraud and cybercrimes. She routinely counsels multinational companies on regulatory compliance matters related to anti-corruption and anti-bribery laws (US Foreign Corrupt Practices Act, UK Bribery Act and local anti-corruption requirements), antitrust and competition laws, cybersecurity and data privacy laws, anti-money laundering legislations, and trade compliance.

Dora has represented multinational clients in many high-stake government investigations by the United States (Department of Justice, Bureau of Industry and Security, and the Securities and Exchange Commission), China and European authorities. She also has extensive experience advising top management on crisis management and complex dispute resolution.

Michael Lowell
Reed Smith

Mike is the co-chair of Reed Smith's global regulatory enforcement group and a member of the firm's global leadership team. He is a leading lawyer in the firm's international trade and national security group.

He has an international practice representing clients on trade and regulatory enforcement matters, including export controls, economic sanctions, anti-bribery and other laws governing cross-border transactions. Mike advises multinational companies from a wide range of industries, including financial services, defence and aerospace, manufacturing, life sciences, and energy and natural resources.

Peter Witherington
Reed Smith

Peter is an associate with Reed Smith's global regulatory enforcement group. His practice focuses on corporate investigations, anti-bribery and antitrust compliance, cross-border regulatory and compliance matters, data privacy, and other general compliance issues. Prior to joining the firm, Peter worked as an associate with another international law firm.

Jessica Tian
Reed Smith

Jessica is an associate in Reed Smith's global regulatory enforcement group in China and Asia. Her practice focuses on regulatory and compliance matters, internal investigations, data privacy and other compliance requirements with respect to anti-corruption and anti-bribery laws (such as the Foreign Corrupt Practices Act, UK Bribery Act and other anti-corruption laws).

Prior to joining Reed Smith, Jessica was a US-trained litigator focusing on employment litigation, including but not limited to ethics and compliance issues and employee disciplines.

ReedSmith

Driving progress through partnership

The strong relationships we build with leading international businesses – from *Fortune 100* corporations to emerging enterprises – help us develop a deep understanding of the outcomes they need to achieve. With teams that are culturally adept and collaborate across geographies, every piece of our legal advice is tailored for the job at hand.

We work to help our clients' business objectives because we get straight to the heart of the matter: to understand what our clients are trying to achieve and what we need to do to help them achieve it. Our structure, processes and use of technology ensure that dynamism is balanced with deliberation – we judge ourselves not on speed, but on getting to the right outcome as efficiently as possible.

An established global law firm, we are based in 29 offices across the United States, Europe, the Middle East and Asia. We understand international business customs, practices and unique laws as well as the different cultures and regulations faced by clients in their markets. Strong relationships with these clients are a result of our ability to speak their languages.

By listening to our clients and mapping their needs, we have developed an industry-focused model that forms part of our strategic philosophy. We now focus, in part, on five key industry groups – each comprising multidisciplinary practices – including energy and natural resources, entertainment and media, financial services, life sciences and healthcare, and transportation.

52nd Floor, Wheelock Square
No. 1717 Nanjing Road West
Jing An District
Shanghai, 200040
China
Tel: +86 21 6032 3188
Fax: +86 21 6032 3199

www.reedsmith.com

Dora W Wang
dwang@reedsmith.com

Michael Lowell
mlowell@reedsmith.com

Peter Witherington
pwitherington@reedsmith.com

Jessica Tian
jtian@reedsmith.com

The *Asia-Pacific Investigations Review 2020* contains insight and thought leadership from 37 pre-eminent practitioners from the region. Across 16 chapters, spanning around 200 pages, it provides an invaluable retrospective and primer.

Together, these contributors capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic. This edition covers Australia, Cambodia, China, Hong Kong, India, Indonesia, Laos, Myanmar, Singapore, Thailand and Vietnam in jurisdictional overviews. It also looks at the impact of AI, data privacy, forensic accounting and law enforcement in multi-jurisdictional investigations.

Visit globalinvestigationsreview.com
Follow @GIRAlerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-225-1