Global Perspectives

International Trends in Commercial Disputes

October 2021

ReedSmith

Driving progress
through partnership

Note from the Editors

Welcome to the October 2021 edition of our Global Perspectives publication.

We are in the fourth quarter of a year that has been marked by geopolitical strife, and the uncertainties presented and compounded by COVID-19, but one that has also seen the continued advance and central importance of technology and data.

While these issues have undoubtedly made an impact on the disputes landscape, corporations and individuals continue to display an indomitable spirit, tapping into reserves of resilience, and facing the unknown with a relative degree of preparation, confidence and hope.

In this issue, our contributors, all leading practitioners located in Reed Smith offices globally, explore a range of current topics seeing interest and action in the disputes universe. They consider the rise of the Metaverse and its relevance to us all. They explore Singapore, Hong Kong and UK issues relating to cryptocurrency fraud and the remedies available to victims and the impact on organizations involved in crypto infrastructure. Our contributors also comment on the importance and status of medical information in a workplace context, highlighting the challenges around COVID-19 testing and vaccination issues in both the UK and the U.S. This edition also takes a look at the use of biometrics and the applicable laws and regulations that govern them in the U.S. and the EU.

We hope there's something in this assortment of topics you find interesting and, of course, wish you all continued health and success in the times ahead.

For more information on these topics, please refer to our virtual conference, Global Disputes in 2021 – A Renewed Perspective.

Our three-day virtual conference explores how people and companies have responded to the pandemic, and discusses what challenges still lie ahead. Companies have gone from reopening to re-evaluating, as the Delta variant, together with vaccine unavailability and hesitancy related issues, forces companies to delay return-to-work plans. Innovative ways of doing business unfortunately are opening the door to bad actors who insinuate themselves by penetrating weaknesses in cybersecurity protections and wreak havoc. Plus, evolving dispute resolution methods are giving rise to new considerations for companies, especially when litigating and arbitrating across borders.

Reed Smith disputes lawyers and guests, including Alex Kazan and Lucy Eve of Eurasia Group, Jean Lee of the Minority Corporate Counsel Association, Katie Pavlovsky from Deloitte and Klaus Reichert, QC from Brick Court Chambers, discuss key issues impacting corporations and the global disputes landscape.

Watch the program here: Global Disputes in 2021 - A Renewed Perspective.

Douglas E. Cherry
Editor
Partner, London

Karen A. Braje
Editor
Partner, San Francisco

Cryptocurrency fraud: Singapore and Hong Kong routes to obtaining information

Fraud is a global growth industry that has infamously enjoyed a period of expansion during the current COVID-19 pandemic. Bad actors may be opportunistic and premediated in their approach. As financial systems change and evolve, so too do the mode and manner of the nature and the targets of their fraud. The evolving and ever-changing world of cryptocurrencies as a means of representation of value, payment or an investment product presents new opportunities to criminals and risk to "market" participants.

Where there is fraud, there will be enforcement by responsible authorities and litigation between parties. In litigation, information is power, and obtaining relevant information in a cryptocurrency fraud is one of the most critical elements in tracing and recovering impacted cryptocurrency. While information may be obtained through the Internet or other technical means, it is often the case that vital information is privately held by entities, including cryptocurrency exchanges. Given the need to have information sufficient to sustain a litigation claim, it is important to understand how parties can gain access to that information.

We look at the recent case decided by the High Court of England and Wales of *Fetch.ai Limited & Anor v. Persons Unknown & Ors* [2021] EWHC (Comm) 2254, which provides useful insight into the importance of information and how to get it.

Fetch.ai fraud

The claimants discovered that their accounts holding cryptocurrencies with Binance Holdings Limited (a Cayman entity) had been compromised. These accounts held various amounts of different cryptocurrencies, including USDT, BNB, BTC, and FET. The fraudsters then operated those compromised accounts, trading the cryptocurrencies at a significant undervalue to anonymous third parties over a very short period of time, resulting in a loss to the victims of more than US$2.6 million.

Why England and Wales?

The High Court spent some time considering which law governed the jurisdiction of cryptocurrency. This was significant as there was no decided English precedent on that point. Ultimately, in the absence of other countervailing authority, the court held that choice of law should be determined upon the fact that Fetch.ai Limited was incorporated in England.

The choice of jurisdiction is often an essential factor in litigation strategy, and in this case, the second claimant, Fetch.ai Foundation Limited, was incorporated in Singapore. Had the claimants so chosen, it is possible that Singapore might have had jurisdiction. Ultimately, the centrality and certainty of English law in this matter appears to have been preferred, and the matter proceeded in the English court.

Persons unknown

Given the nature of the fraud, it should not come as a surprise that the Fetch.ai case is against "Persons Unknown." English law has long established the practice and principle[1] allowing claims to be brought against categories of "Persons Unknown" since victims of fraud may not know the precise identity of the perpetrators.

Similarly, Hong Kong has readily adopted the same practice[2] to enable orders against anonymous persons interfering with victims' rights. Although there has been no reported case in Singapore confirming the same approach, we believe it is highly likely that the Singapore courts have the authority to allow such claims.

On its face, it may seem illogical to commence a claim against persons unknown, as without a defendant, the hope of recovery is impaired. There is, however, method in doing so because it allows information to be gathered, which further assists in the formulation and sustaining of the claims and also facilitates the prospect of obtaining information and other remedies from third parties.

In the Fetch.ai case, the claimants sought a host of remedies including injunctive relief, worldwide asset freezing orders, and related orders seeking disclosure of information against the unknown fraudsters as well as the recipients of the cryptocurrency sold by the fraudsters. They also sought Bankers Trust and Norwich Pharmacal orders against Binance Holdings Limited (the second respondent) and Binance Markets Limited (the third respondent), as the cryptocurrency exchange parties.

Critical information sought by the claimants

The claimants wanted to obtain significant critical information from the Binance entities, including customer personal data relating to the accounts that received the "benefit" of the undervalued trades. IP addresses would also be obtainable if the fraudsters had been careless about accessing the claimants' trading accounts. In combination, this information could lead to the location and preservation of the misappropriated cryptocurrencies.

In granting a Bankers Trust order against the Binance respondents, the High Court in *Fetch.ai* considered the following:

1. There were good grounds to conclude that the cryptocurrencies originally belonged to the claimants. This is usually not hard for claimants to prove.
2. In answering the question as to whether there was a real prospect that the information sought would lead to the location or preservation of the misappropriated cryptocurrencies, the court held there was. It held that a strong inference could be drawn that the Binance respondents had such relevant information (that is, the personal data of their own customers) and that this information could be used to locate and preserve assets.
3. The court was satisfied that the order sought was not unnecessarily broad. We note that this issue is largely a legal drafting point, but the key point is to ensure that the wording of the order receives the proper attention it needs in order to be successful under the circumstances. The key point is not to overreach in a request for information.
4. The fact that a fraud had already occurred weighed heavily in favor of the victims when the court assessed the balance of convenience in deciding whether to make the Bankers Trust order. The court also considered Binance's terms of use, which themselves did not preclude Binance from disclosing customer information if compelled to do so by a court of competent jurisdiction.

5. The claimants demonstrated to the court's satisfaction that they retained assets of more than £150 million, which meant that they could meet their undertaking as to damages and also any expenses incurred by the Binance respondents in giving disclosure as sought. This was an important factor for the court, as it meant that even in the worst-case hypothetical scenario, if the claimants were entirely wrong to pursue their claim, the respondents would be able to pursue the claimant for damages suffered due to the order as sought being made and complied with by the respondents.

The court also considered granting a Norwich Pharmacal order, which would have resulted in compelling the Binance respondents to disclose the same information. Although the considerations were slightly different, they are similar, and the court ultimately granted the disclosure order:

1. There was a wrong carried out by an ultimate wrongdoer;
2. The disclosure order would enable action to be brought against the ultimate wrongdoer;
3. The Binance respondents, though not parties to the wrongdoing, were "mixed up" in it and likely to have information necessary to identify the ultimate wrongdoer; and
4. The disclosure order was a necessary and proportionate response in all the circumstances.

Considering the position in Hong Kong and Singapore in light of the English court's decisions

In Hong Kong, the considerations for a Bankers Trust order[3] and a Norwich Pharmacal order[4] are very similar to the English law position as set out above. The weight given to any one consideration may vary, but the relevant factors for consideration are the same.

In Singapore,[5] however, the requirements for granting a Bankers Trust order or a Norwich Pharmacal order are less stringent than the test in *Fetch.ai.* The following three main criteria must be satisfied:

1. The person possessing the information sought must have been involved in the wrongdoing;
2. There must be a real interest and need for an order to enable action to be brought against the ultimate wrongdoer; and
3. It is necessary, just, and convenient to order the disclosure of the relevant documents.

The three jurisdictions are more similar than they are different, which must be encouraging in cases of cryptocurrency fraud. The nature of the currencies themselves are typically borderless and ethereal in nature, so consistency in how legal systems may tackle the issue of fraud across global boundaries is good. It streamlines the ability to understand the issues, highlights differences, and allows claimants to act swiftly and with clarity in formulating their legal approach and litigation strategy and implement it without delay.

Closing thoughts

In the battle against cryptocurrency fraud, information is key.

Delay is an enemy of success in cases of cryptocurrency fraud.

Even when the perpetrators of a fraud are unknown, swift steps can and should be considered to preserve the position, and stem the tide of any ongoing fraud.

The imbalance of information in cases of fraud is daunting, however, it is important not to underestimate the type of information you can obtain from available court-ordered remedies, as we see in *Fetch.ai*. The information gained from such orders may not immediately result in recovering the stolen assets or finding the fraudsters, but is – at the very least – a step on the path to success.

Click here to read our recent alerts on the issue of cryptocurrency fraud.

Reed Smith LLP is licensed to operate as a foreign law practice in Singapore under the name and style, Reed Smith Pte Ltd (hereafter collectively, Reed Smith). Where advice on Singapore law is required, we will refer the matter to and work with Reed Smith's Formal Law Alliance partner in Singapore, Resource Law LLC, where necessary.

Authors:

Stephen Chan
Partner, Hong Kong

Fiona Leung
Associate, Hong Kong

Hagen Rooke
Counsel, Singapore

Timothy Cooke
Partner, Singapore

Doug Cherry
Partner, London

Biometrics: The litigation and regulatory landscape

As businesses use ever-increasing amounts data – for employees, customers and vendors – biometrics have become a hot topic among businesses, regulators, and lawmakers alike. Many lawmakers are focused on limiting or preventing the use and/or transfer of biometric data, which can result in significant penalties for companies that are not in compliance. It is critical that organizations that use or seek to use biometrics be aware of the applicable laws and regulations. Our Biometric Team routinely assists clients, across varying industries, navigate the patchwork of regulations and laws that govern (in the U.S. and abroad) the use of biometrics, including regulatory counseling and defending against putative class actions.

What Are Biometrics?

Biometrics refer to unique physical characteristics that can be used to identify a particular person, such as a fingerprint, iris scan, voice print or even an individual's DNA. Biometric markers can be used for security purposes (*e.g.*, to confirm a person's identity) or for convenience (*e.g.*, to identify you and others in photos). Biometrics often might seem to be more science fiction than reality. For example, consider Hollywood depictions of biometrics that include *Minority Report* (set in a dystopian future where advertisement billboards can track you, identify you in a split second, and advertise to your specific interests as you walk by). But in reality, biometrics are used far more often than many people realize. The cellphones that we carry in our pockets often request our biometric information (either a facial scan, iris scan, or a fingerprint scan) to provide a secure and convenient way to unlock the phone, pay for items or access sensitive information. Similarly, security cameras are paired with facial recognition software to identify a person in a crowd, and DNA is used to identify family members and solve crimes.

What sets biometrics apart from more popular means of identification (*e.g.*, names, usernames and passwords, social security numbers, etc.), is that biometrics are nearly impossible to change. Security measures that incorporate biometrics tend to be more secure and convenient than standard username and password combinations because once that information is captured or compromised, there is little one can do to "re-secure" the relevant identifier. Depending on the motives of the person or organization that has access to the biometric data, the data can be used to carry out targeted tracking and/or identity theft.

A Patchwork of Laws and Regulations Govern Biometric Use

Because biometrics are unique identifiers, regulators and lawmakers are concerned about these identifiers falling into the hands of bad actors or being abused by companies. However, in the U.S., the applicable laws vary from jurisdiction to jurisdiction since there are no applicable federal laws. As a result, a patchwork of laws and regulations regarding biometrics have developed, and a number of bills are moving through the legislative process now.

The most notable law governing biometrics is the Illinois Biometric Information Privacy Act (BIPA), which has a broad application and permits private lawsuits for violations that has resulted in an explosion of litigation. BIPA restricts an organization's ability to sell or disclose the biometric information captured and requires opt-in consent to use biometrics for a defined purpose. Failure to comply with BIPA's requirements can result in penalties up to $1,000 for each negligent violation and up to $5,000 for each intentional or reckless violation. Publicly disclosed settlements of BIPA-related class actions have been substantial – $650 million by Facebook (alleged photo tagging), $92 million by TikTok (alleged facial recognition in videos) and $36 million by Six Flags (alleged improper storage of fingerprints).

A growing number of states and cities have some type of law or regulation that governs the use of biometric information. For example, New York has released a Biometric Identifier Information Law, which brings with it a private right of action. *See* *New York City releases a new biometric law bringing with it a private right of action*, Reed Smith Client Alerts, June 17, 2021. There are more laws and regulations on the way, which will add further complexity to the current patchwork.

Outside of the U.S., countries have taken different approaches to regulating biometric use. For example, the European Union, through the European Data Protection Board and the European Data Protection Supervisor, has called for a ban on nearly all use of AI-driven biometric identification in public places, while the United Kingdom has taken a less stringent approach (permitting the use of facial recognition, with a very high threshold prior to the roll out of any technology).

What's Next?

Although the legal and regulatory framework governing biometrics is rapidly expanding (and in inconsistent ways), the use of biometrics by businesses and consumers continues to grow because the security and convenience value is undeniable.

Organizations that use biometrics, and, most critically, that rely on biometrics to generate significant revenue should pay close attention to proposed (and new) legislation and trending issues in the regulatory and class action litigation space.

Authors:

Geoff Young
Partner, New York

Natsayi Mawere
Associate, New York

Michael Galibois
Partner, Chicago

Dr. Andreas Splittgerber
Partner, Munich

The Metaverse is here: Is your company ready?

By nature, lawyers are curious, eager to learn and react to new ways of doing things. The law is precedential, built on a foundation of prior experience; the result of centuries of human behavior and the reactions and influence of governments and lawmakers. The concept of the metaverse is, therefore, naturally seductive to lawyers. It is a new world, an evolving, alternative digital environment. Driven by the dramatic evolutionary combination of technology, devices, and communication networks, the metaverse offers human beings the opportunity to collaborate, transact, perform, argue, and create as never seen before in history. It enables our alternative selves.

There is no doubt that the metaverse is a critically important consideration and influence. People exist there and there is money to be had. Deciphering the law pertaining to these online environments and advising companies who operate in them will require both a strong handle on legal precedent and an open mind.

The next advent of the metaverse and decentralized features of what is known as the Internet 3.0 offers tremendous opportunities for growth. The entertainment and media sector is at the cutting edge, but the rest of the commercial world is close behind: healthcare, finance, energy, logistics and even traditional manufacturing industries will be affected by what's happening in these online environments.

What is the metaverse?

The word means "beyond the universe," but what exactly is the metaverse? One way to describe it is the increasing permeability of the borders between digital environments and the physical world.

Imagine stepping into a cyberworld: the metaverse is a space where you can interact with virtual objects in real life with real-time information. It is likely that you have already seen this concept in movies and on television programs – for instance, Iron Man,[6] Ready Player One,[7] and Upload.[8]

Adopting this literal approach to the metaverse means it is a combination of three elements. First, it is a technology that enables digital content to be laid over the real world, similar to augmented reality (AR). An example is the smartphone game, Pokémon Go. Digital content is combined with the real world. Second, the metaverse applies a hardware device that enables the real world to be interactive. Digital content is applied so that users can control content displayed virtually and interact with it within a real-life space. Third, it is information about anything and everything in the physical world (an area, a shop, or a product) and knowledge about the user (the user's schedule, location, habits, and interests). This information will be obtained from the Internet and from machines learning about a user's everyday actions. A simple example of a device learning based on a user's everyday activities is Siri (on iOS) or Alexa (on Amazon). Real-time information is obtained instantly and virtually, while in the background data is being collated and applied.

However, modern-day gaming environments have moved the metaverse far beyond the clunky, often avatar-limited 3D block worlds into entirely new, ever-evolving creative online habitats. The critical difference between the metaverse then and the metaverse now is a user's ability to create. Games such as Minecraft, Roblox and Fortnite have changed the way we think about being online. Parents wonder why their children spend so long in these metaverse worlds, and it is because people are interacting, creating and entertaining each other. Mini-industries have evolved and exist around these worlds; people are paid in the real world to create virtual products on Minecraft and rock stars vie to perform virtually on Fortnite. Millions of people participate in events that happen only in these metaverse environments.

What are the commercial applications of the metaverse, and who will benefit from it?

The metaverse will alter the way we act, socialize, work, and live. We discuss some commercial applications here, but there are business opportunities for participants in every sector. Purchasing items can be instantaneous. When you see a product in a store or on the metaverse, you will not need to open an app or even touch your smartphone. Products can be purchased and prices can be compared through one account and in one place. This means that goods will be more accessible, and businesses will be able to sell their goods worldwide.

Ultimately, consumers will gain most as information, products, entertainment, and social experiences are enhanced and more accessible. The reach, immediacy, and interactivity for businesses and celebrities will be significantly increased, with greater opportunity for collaboration. The capability to offer richer, more targeted commercial promotions to consumers will increase and consumers will be able to interact with brands directly, thereby increasing user engagement will be higher.

There will be further emphasis on digital goods and property such as non-fungible tokens (NFTs). Items that can be traded can become more marketable because they are not prone to wear and tear. For gaming, the players can expect more interactive experiences. An item or skin purchased in one game may be used in another game or may be traded. As the way we work and socialize changes, there will be new ways to monetize, in particular in media, social media, technology, and retail. Hardware technology companies and software companies will dominate the market as demand increases.

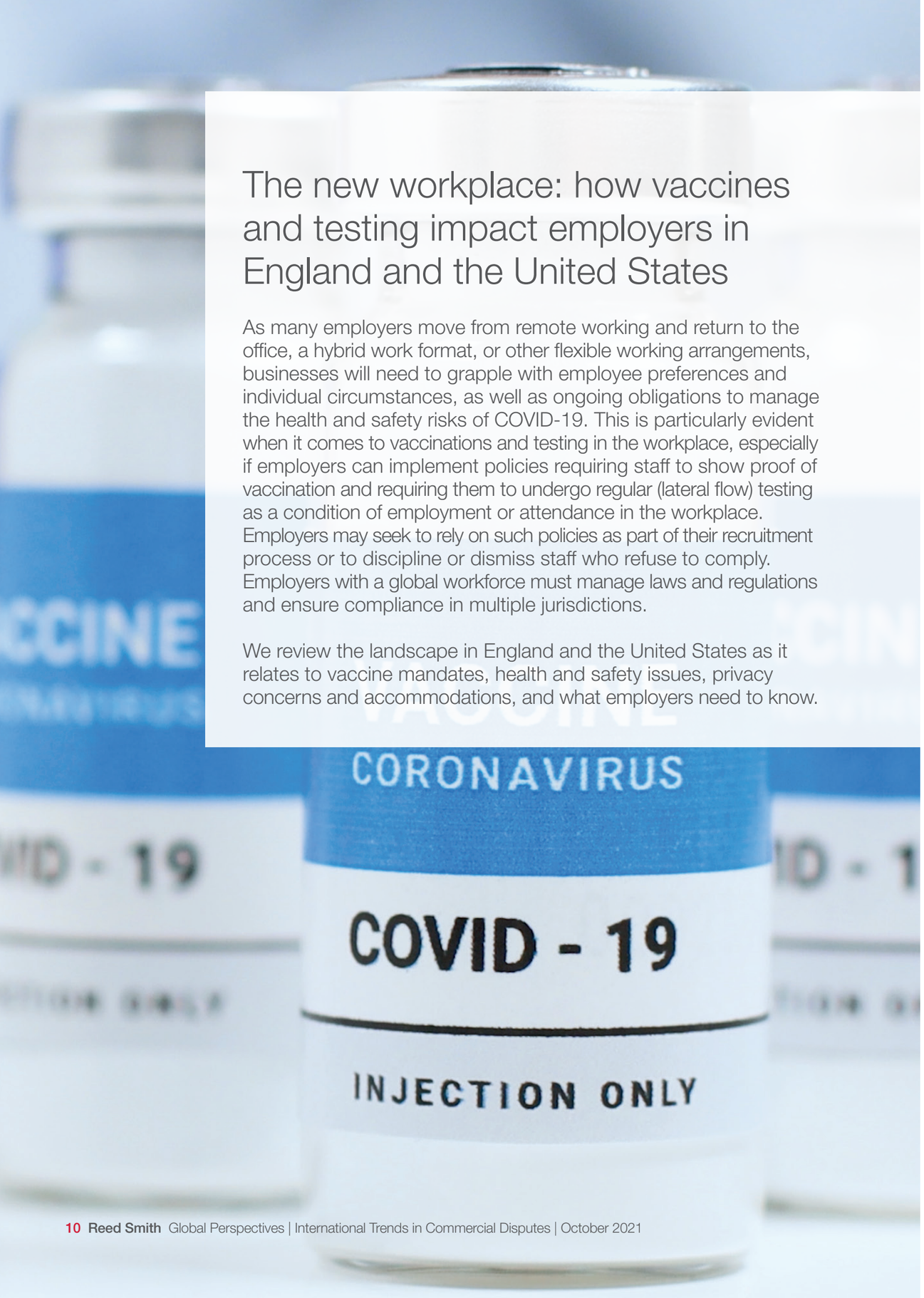
There is no general consensus on how the metaverse will work in the future, or who will build it or who will "own" it (if anyone). So what does this mean? There will be a need for legal advice due to the uncertainty of the law and regulations – in the areas of data protection, privacy, and advertising regulations and to ensure that commercial intellectual property assets are protected as the virtual and real world converge. This need to ensure that real-world laws are effectively translated into the virtual world will continue to challenge lawyers and lawmakers.

Click here to read an overview of some of the legal issues arising from the metaverse.

Authors:

Gregor Pryor
Partner, London

Stephen E. Sessa
Partner, Century City



The new workplace: how vaccines and testing impact employers in England and the United States

As many employers move from remote working and return to the office, a hybrid work format, or other flexible working arrangements, businesses will need to grapple with employee preferences and individual circumstances, as well as ongoing obligations to manage the health and safety risks of COVID-19. This is particularly evident when it comes to vaccinations and testing in the workplace, especially if employers can implement policies requiring staff to show proof of vaccination and requiring them to undergo regular (lateral flow) testing as a condition of employment or attendance in the workplace. Employers may seek to rely on such policies as part of their recruitment process or to discipline or dismiss staff who refuse to comply. Employers with a global workforce must manage laws and regulations and ensure compliance in multiple jurisdictions.

We review the landscape in England and the United States as it relates to vaccine mandates, health and safety issues, privacy concerns and accommodations, and what employers need to know.

The landscape in England

COVID-19 vaccines in England

There is currently no law in England mandating that employees working outside of the regulated care industry be vaccinated in order to perform their duties, nor is there anything more than a strong recommendation that individuals undergo regular lateral flow tests to avoid the spread of the virus. The decision to mandate vaccinations or testing as a condition of employment or attendance at the workplace is left to employers. This differs from the rules in the U.S., which we address in an adjoining article.

This is an evolving area, and there are inherent risks for employers who are looking to require that their employees be fully vaccinated, tested, or both as a condition of employment or of being present at the business premises absent legislation. Employers will need to account for a variety of factors, including their health and safety obligations, employment law and employee relations issues, as well as data protection considerations when deciding how to proceed.

Health and safety considerations

In consultation with staff or health and safety representatives, employers should be assessing the risk in the workplace and putting reasonable and appropriate measures in place to mitigate the exposure to COVID-19 generally.

Government guidance recommends, as a minimum, focusing on things like cleaning, ventilation, social distancing, and reducing contact. Guidance also identifies other appropriate measures that can be taken: tracking employees who enter office premises (this can be done via online questionnaires or logbooks); and requiring staff to declare that they do not have symptoms, have not had a positive test result, and – before entering the workplace – have not had contact with someone who has tested positive for COVID-19. Government guidance also advises encouraging staff to take personal responsibility for themselves and others when making decisions about attendance.

This guidance does not refer to the introduction of mandatory vaccine requirements or regular testing when discussing appropriate measures that employers may take to make workplaces safe. This is a surprising omission and seems to ignore the role that vaccination plays in enabling workplaces to reopen, as well as the value of testing. It also does little to alleviate uncertainty for employers since implementing mandatory vaccination or regular testing requirements is not rendered unlawful by their omission from the guidance but is not clearly supported either. However, what can be understood from the guidance is that vaccination and testing requirements are not in themselves an answer to securing the workplace. Where such requirements are to be implemented, they must build upon the other measures set out in the guidance but not replace those other measures.

Including requirements within the employment contract

The employment contract is a key document, setting out terms and conditions of employment and the consequences of noncompliance. Employers may, therefore, consider using this as a place to set out their vaccination and testing requirements. For new hires in particular, continued employment could be made conditional (at least from a contractual perspective) upon meeting those requirements. If considering this step for new hires, employers would still need to be mindful of discrimination risks and data protection considerations, both of which are discussed in further detail below. Unfair dismissal risks would also remain relevant once the employee has reached the two years of continuous service necessary to be able to bring such a claim.

In relation to an existing workforce that has already entered into employment contracts, individual employee consent would be needed in order for new terms concerning vaccination and testing to be incorporated. Accordingly, a move to introduce new terms and conditions could become challenging where employee agreement is not forthcoming and an employee relations problem emerges. As a potential way forward from such an impasse, the employment contracts of those who do not agree to the vaccine and testing requirements could be terminated with an offer of new terms that contain those requirements. However, this could prove to be quite a complicated and, potentially, risky strategy. Depending on the numbers involved, collective consultation requirements could be engaged, and there is always the prospect of dismissal-related claims from those who choose not to sign up to the new terms. A very careful analysis of the workforce's likely response should, therefore, be carried out in advance of taking action.

Unfair dismissal risks

At the time of writing, there have been no Employment Tribunal decisions providing guidance on the approach that might be taken in the event of an unfair dismissal claim by someone who is terminated for not meeting vaccine or testing requirements. For employers with an established workforce, this makes the potential outcome of imposing such requirements uncertain, as it is difficult to predict how any consequential unfair dismissal claims would be dealt with.

In order to defend an unfair dismissal claim, an employer must be able to demonstrate that a "potentially fair" reason for dismissal existed and that it was reasonable to have dismissed for that reason. Commentators seem to agree that two of the five statutorily prescribed fair reasons for dismissal – namely conduct and "some other substantial reason" – may be applied to a dismissal for noncompliance with vaccine or testing requirements. However, whether it is reasonable to dismiss an employee for those reasons should be considered on a case-by-case basis.

With regard to the reasonableness test, employers would likely be required to demonstrate, among other things, the importance of the vaccination and testing requirements to their business and operations. It is also likely that employers would be required to demonstrate that they have also taken other measures to protect against the risk of COVID-19 and are not seeking to rely solely on the vaccine. This again underscores the importance of using vaccination and testing requirements as part of a strategy for managing the COVID-19 risk and not as a replacement for other steps.

Employers also need to be mindful of the potential unfair dismissal risk when dealing with those who object to returning to the workplace due to health and safety concerns (for example, if an employee refuses to return to the workplace if colleagues are not vaccinated). If the employee can demonstrate that they have a reasonable belief of a serious and imminent danger to health and safety and has not returned to work for this reason, dismissal would give rise to an automatic unfair dismissal. Employers will therefore need to deal with such circumstances carefully. It also underlines the need to put in place a comprehensive set of measures to put employees' minds at rest and mitigate against the possibility of any employees forming a belief (reasonable or otherwise) of danger from a health and safety perspective.

Discrimination risks

Job applicants and employees of any length of service are able to bring discrimination claims. The Equality Act 2010 covers those with protected characteristics (as defined under the Act) from being treated less favorably as a result of those characteristics. The application of a broad-brush policy mandating the vaccine and regular testing for the purposes of receiving a job offer, ongoing employment, or attending the workplace, can potentially be argued as constituting discrimination, unless the employer can objectively justify its approach.

The protected characteristics of particular relevance to this debate and where there may be an inability or unwillingness to receive the vaccine are disability, religion or belief, race, and pregnancy.

- Disability discrimination: Individuals with certain disabilities may be unable to get the vaccine.
- Religion and belief discrimination: Some people may practice a religion that prevents them from receiving the vaccine (for example, by reason of the vaccine containing products forbidden by the candidate's faith). Others may have a moral or other belief system under which they are opposed to the vaccine (for example, those considered "anti-vaxxers" (albeit this is a broad term, and the onus would be on the candidate to demonstrate a genuine belief system in this regard).
- Race discrimination: The statistics suggest that certain racial and ethnic groups are more vaccine hesitant than others.
- Pregnancy/maternity (breast-feeding): Employees may refuse to agree to be vaccinated on the basis that they are pregnant or breast-feeding, especially where guidance is changeable and the effects are not known.

Discrimination risks can be avoided where employers can objectively justify their policy on mandatory vaccines. However, the ability to put in place such justification cannot be guaranteed. The risk could otherwise be mitigated by having some flexibility to take into account the circumstances of individuals who are not vaccinated and permit exemptions from vaccination requirements on a case-by-case basis.

Data privacy issues

Any information that an employer asks its job candidates and staff to provide to confirm COVID-19 test results and vaccine status would constitute "special category personal data" under data protection laws, and so particular care is needed with the processing. To comply with the "data minimization" principle, employers should ask for the minimum amount of data required. Ideally, only a "yes" or "no" response would be given to a question as to whether an individual has been fully vaccinated, rather than actual evidence being stored, and if any further health information is provided (for example, the type of vaccination received), this should be deleted as soon as possible. Further, if an individual has a clinically approved exemption status, the company should not request further information about the clinical reason behind the exemption.

Prior to carrying out any processing of data concerning test results and vaccine status, companies must undertake a Data Protection Impact Assessment (DPIA) given that the processing is of high-risk data. This will need to document, in particular, the reasons for checking or recording people's COVID-19 status since data protection laws would not enable a company to process it on a "just in case" basis. The UK Information Commissioner's Officer has a template DPIA form that can be used.

There must also be a lawful basis for processing the data, and this must be documented. This would likely be "legitimate interests" (requiring the completion of a Legitimate Interests Assessment, which could be done at the same time as and combined with the DPIA). Since health data is being collected, employers can then rely on the protection of the health, safety, and welfare of employees under schedule 1 of the UK Data Protection Act 2018 (often referred to as "the employment condition"). This condition additionally requires that the company have an "appropriate policy document" regarding the processing which is a prescribed form under the legislation.

Companies should also update their privacy notices to staff and candidates to explain the processing of this data and their rights in relation to it. Details should be included in the company's records of processing.

There should be clear protocols and processes in place to ensure that the information is not kept longer than is necessary, that it is only viewed on a need-to-know basis with firm access controls in place, and that it is kept secure.

From a UK GDPR perspective, there is no set retention period for sensitive information, but the general principle is that it should not be kept for any longer than necessary for the purpose for which it was collected. For example, if vaccination status data is kept in order to facilitate international travel, the data should be deleted once the individual has traveled since afterward, it will no longer be needed for the purpose collected.

We hope this summary of the position in England was helpful. For those of you with global operations or who are just curious, we set out a similar analysis in the following article as it applies to the United States.

Authors:

Carl De Cicco
Counsel, London

Elle Todd
Partner, London

Carlene Nicol
Associate, London

Allison Heaton
Knowledge Management Lawyer, London

The U.S. landscape

Mandated vaccination policies in the United States

Generally speaking, U.S. employers can, and may even be required to, implement a mandatory vaccination policy, but there are some key issues employers should consider. In guidance issued in late May 2021, the U.S. Equal Employment Opportunity Commission (EEOC) took the position that mandatory vaccination policies are generally permissible under federal antidiscrimination laws. Just a few weeks later, in June 2021, a U.S. federal court – in the first ruling on this issue – echoed this sentiment in concluding that such policies are generally permissible. The following month, the U.S. Department of Justice issued a detailed memo reaching the same conclusion.

Building off of these developments, on September 9, 2021, President Biden announced several measures intended to expand the use of mandatory workplace vaccination policies amongst United States employers. The measures include: (1) an executive order that requires certain government contractors and subcontractors to mandate COVID-19 vaccinations for their workers; (2) an announcement that the Centers for Medicare & Medicaid Services are taking steps to require vaccinations for workers in health care settings that receive Medicare or Medicaid reimbursements; and (3) an emergency temporary standard (ETS) to be issued by the Occupational Health and Safety Administration (OSHA) that will require all employers with 100 or more employees to ensure their employees are vaccinated or tested weekly for COVID-19. Employers subject to the ETS will also be required to compensate employees for time spent receiving a COVID-19 vaccine or recovering from the vaccine's side effects. While President Biden's measures will face legal challenges, the success of the legal challenges is hard to predict, particularly without the full details of the ETS.

Notably, however, there are limits to the breadth of US workplace vaccination policies. Specifically, employers who implement a mandatory vaccine policy must consider potential accommodations or exceptions to the mandate for employees with disabilities, certain medical conditions, and a sincerely held religious belief, practice, or custom. If an employee requests an exemption from a mandatory vaccination policy on one of these grounds, the employer must engage in the so-called interactive process with the employee and may be required to provide the employee with a reasonable accommodation. In addition to legally required accommodations, the EEOC also cautions employers to be cognizant of any potential disparate impact created by a vaccine mandate.

Additionally, several states have enacted legislation (or, as of this writing, are attempting to enact legislation) that bans employers from imposing vaccine mandates. Most of the bans are limited to employees of state and local governments. The exception is Montana, which has passed legislation that effectively prohibits employers from implementing a mandatory COVID-19 vaccine policy. It is unclear how the Biden Administration's mandates regarding vaccines will interact with state laws prohibiting mandatory vaccination.

Employers must also be cognizant of the potential obligation to pay non-exempt employees for the time employees spend being tested or vaccinated – including any recovery time – pursuant to a mandatory vaccination or testing program.

Employees who will not or cannot get vaccinated

If an employee certifies that they cannot get vaccinated due to a disability, medical condition, or a sincerely held religious belief, the employer must engage in the interactive process with the employee. Based on the information gathered from the employee and the circumstances of the employer, a reasonable accommodation may need to be made. In the context of exemptions from a mandatory vaccination policy, reasonable accommodations could include: (1) minimizing contact with coworkers; (2) eliminating contact with the public; (3) remote working arrangements; (4) alternative safety equipment or personal protective equipment; or (5) reassignment.

If an employee cannot get vaccinated against COVID-19 because of a disability, medical condition, or a sincerely held religious belief and there is no reasonable accommodation possible, then it may be lawful for the employer to exclude the employee from the workplace. This does not mean the employer may automatically terminate the worker, however. Employers will need to determine if any other rights apply under applicable federal, state, or local laws, rules, and regulations. Employers should consult legal counsel before taking any such action.

Absent a medical, disability, or religious exemption from a mandatory vaccination requirement, an employer can make a COVID-19 vaccination a condition of employment and terminate employees who do not comply. Again, employers should tread carefully with this practice and consult legal counsel prior to making any such decisions.

Asking employees about vaccine status or requiring proof of vaccination

Under federal law, a narrow inquiry into whether an employee or job applicant has been vaccinated is generally permissible. However, employers should be mindful of any state or local laws that may restrict such inquiries.

The EEOC has taken the position that simply requesting proof of vaccination is not a prohibited disability-related inquiry under the federal Americans with Disabilities Act (ADA) and is permitted under federal law. However, subsequent employer questions, such as asking why an individual did not receive a vaccination, may elicit information about a disability and would be subject to the pertinent ADA standard that inquiries be "job-related and consistent with business necessity." Employers also should be mindful that asking about the vaccine status of an employee's family members may implicate the federal Genetic Information Nondiscrimination Act (GINA). Additional state and local laws may also apply.

Confidentiality and privacy concerns regarding vaccine status and related information

Employers are required to keep all information about their employees' vaccination status confidential. Additionally, all employee vaccination records (and related information) must be kept separate from employee personnel records. Companies should be mindful of what information they are requesting because the inquiry might trigger heightened data-privacy and document-retention requirements. Companies should request only the information they require to confirm the vaccination status of the employee and should not collect any other information that is not necessary for that purpose.

Additionally, companies should be mindful of the privacy, security, and other legal requirements involved in communicating with employees about any requested exception to a mandatory vaccine program based on a medical condition. The interactive process would likely include asking employees disability-related questions – and potentially questions implicating genetic nondiscrimination and health data privacy laws (such as GINA or the Health Insurance Portability and Accountability Act (HIPAA)).

Employers also should consider how they plan to receive such information, and what they will do with it once they have it. Questions to consider include:

- How secure is your company's email system?
- Can employees access their work email on their phones? If so, are there password and other security measures in place to prevent unauthorized access to that information?
- What does HR plan to do with the information once it receives it? Will it be printed out and stored in a paper file?
- Does the company plan to insert that information into the employee's personnel file or HR database?
- Who would have access to that information?
- If the company plans on storing the data electronically, does the company have sole possession, custody, and control of the servers where the data will be stored? If so, the company may want to confirm where those servers are physically located, and whether any state or local laws of that jurisdiction impose additional data-privacy, data-security, and breach-notification requirements. If an employer plans to contract with a third party to maintain that information, it presents a whole other host of issues that must be navigated.

What about employees who refuse to return to the workplace?

This is one of the most frequently asked questions about reopening workplaces. Employers should approach each situation individually. Factors employers should consider include: the employee's duties, work location, industry, vaccination status, current COVID-19 transmission levels, and workplace safety efforts. Generalized concern about the virus – without more – is not legally protected under federal law. Nevertheless, employers should consider – subject to any individualized considerations warranted by the particular situation – educating the employee about, among other things, the company's health and safety protocols before considering an adverse action like termination.

Additionally, if an adverse action is taken against the employee, the employer may want to consider an action short of termination (for example, a leave of absence, short-term transfer to a different role that allows remote working, etc.). Overall, employers should tread carefully and exercise a measure of flexibility when considering adverse action to an employee's refusal to come to work due to generalized concerns about the virus.

Click here to read more frequently asked questions on US employee privacy issues related to the COVID-19 vaccine.

Authors:

Sarah Bruno
Partner, San Francisco

Mark Goldstein
Partner, New York

Amanda Brown
Senior Associate, Dallas

Michael Lombardino
Senior Associate, Houston

Endnotes

Cryptocurrency fraud: Singapore and Hong Kong routes to obtaining information

1 *Bloomsbury Publishing Group PLC & Anor v. News Group Newspapers Ltd. & Ors* [2003] EWHC (Ch) 1205.
2 *Billion Star Development Limited v. Wong Tak Cheung*, [2012] 2 H.K.L.R.D. 85.
3 *Pacific King Shipping Holdings Pte. Ltd. v. Huang Ziqiang*, [2015] 1 H.K.L.R.D. 830.
4 *A1 & Anor v. R1 & Ors*, [2021] H.K.C. 650 [C.F.I.].
5 *La Dolce Vita Fine Dining Co. Ltd. and another v. Deutsche Bank AG* [2016] SGHCR 3.

The Metaverse

6 https://www.youtube.com/watch?v=Ddk9ci6geSs
7 https://www.youtube.com/watch?v=cSp1dM2Vj48
8 https://www.youtube.com/watch?v=0ZfZj2bn_xg

Authors

Sarah L. Bruno
Partner, San Francisco
+1 415 659 4842
sbruno@reedsmith.com

Amanda E. Brown
Associate, Dallas
+1 469 680 4232
aebrown@reedsmith.com

Stephen Chan
Partner, Hong Kong
+852 2507 9746
stephen.chan@reedsmith.com

Douglas E. Cherry
Partner, London
+44 (0)20 3116 3837
dcherry@reedsmith.com

Timothy Cooke
Partner, Singapore
+65 6320 5351
tcooke@reedsmith.com

Carl De Cicco
Counsel, London
+44 (0)20 3116 2892
cdecicco@reedsmith.com

Michael B. Galibois
Partner, Chicago
+1 312 207 2810
mgalibois@reedsmith.com

Mark S. Goldstein
Partner, New York
+1 212 549 0328
mgoldstein@reedsmith.com

Alison Heaton
Knowledge Management Lawyer
Global Solutions – Leeds
+44 (0)11 3341 5021
alison.heaton@reedsmith.com

Fiona Leung
Associate, Hong Kong
+852 2507 9805
fiona.leung@reedsmith.com

Michael J. Lombardino
Associate, Houston
+1 713 469 3648
mlombardino@reedsmith.com

Natsayi Mawere
Associate, New York
+1 212 549 4660
nmawere@reedsmith.com

Carlene Nicol
Associate, London
+44 (0)20 3116 3542
cnicol@reedsmith.com

Gregor Pryor
Partner, London
+44 (0)20 3116 3536
gpryor@reedsmith.com

Hagen Rooke
Counsel, Singapore
+65 6320 5363
hrooke@reedsmith.com

Stephen E. Sessa
Partner, Century City
+1 310 734 5426
ssessa@reedsmith.com

Dr. Andreas Splittgerber
Partner, Munich
+49 (0)89 20304 152
asplittgerber@reedsmith.com

Elle Todd
Partner, London
+44 (0)20 3116 3532
etodd@reedsmith.com

Geoffrey G. Young
Partner, New York
+1 212 549 0323
gyoung@reedsmith.com

Phone: +44 (0)20 3116 3000
Fax: +44 (0)20 3116 3999
DX 1066 City/DX18 London

As the seventh largest global litigation firm in the world, Reed Smith has more than 1,000 litigators who have garnered a reputation for comprehensive and international counsel and representation of Fortune 500 and global multinationals in a number of industries, including financial services, life sciences and health, energy and natural resources, media and entertainment, and transportation. Reed Smith is on hand to help you achieve solutions that are right for you.

ABU DHABI
ATHENS
AUSTIN
BEIJING
BRUSSELS
CENTURY CITY
CHICAGO
DALLAS
DUBAI
FRANKFURT
HONG KONG
HOUSTON
KAZAKHSTAN
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

reedsmith.com