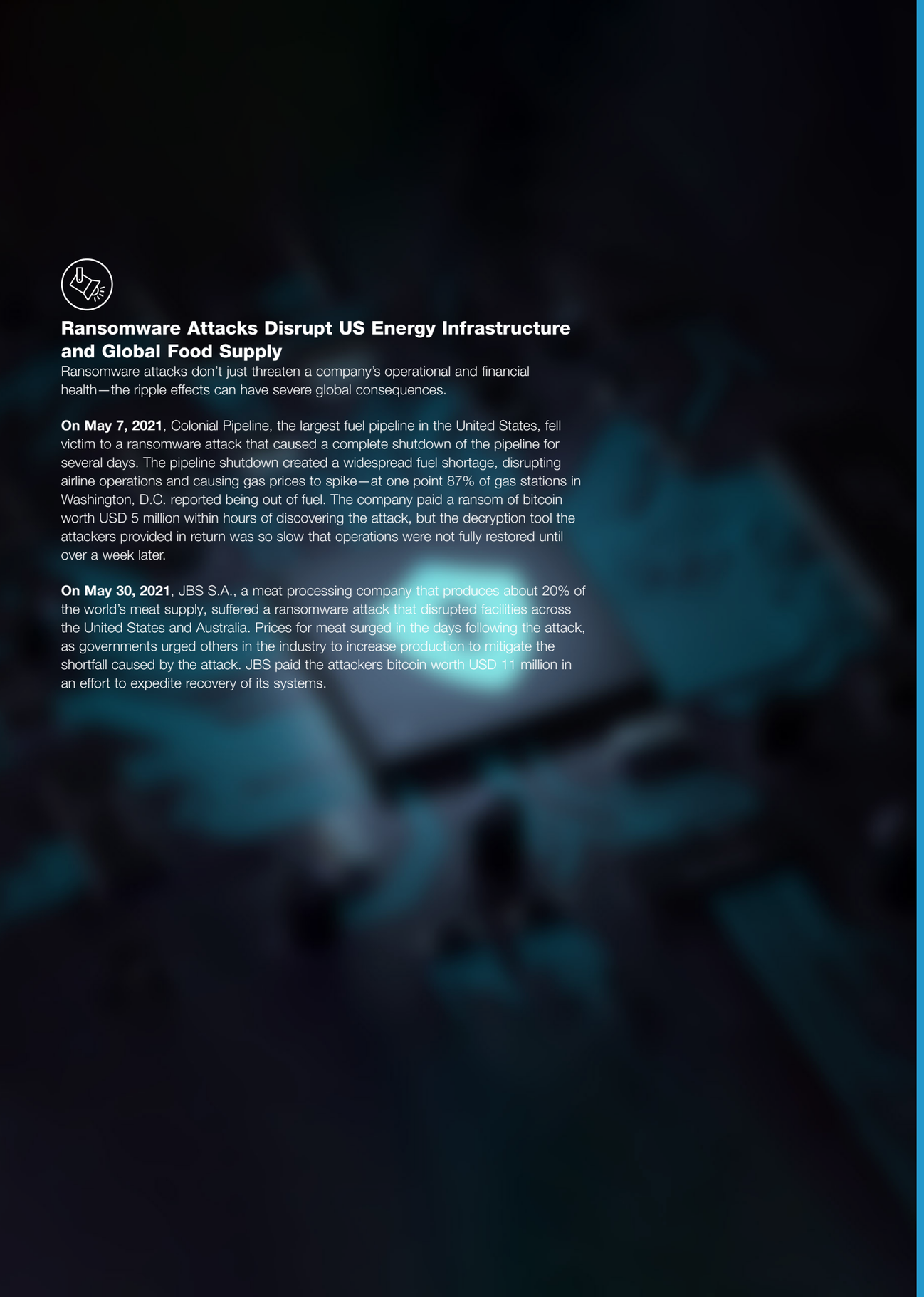
CLIFFORD

CHANCE

RANSOMWARE: PREVENTION & RESPONSE

UNDERSTANDING THE RISKS AND HOW TO ADDRESS AN ATTACK

Q1 2022



Ransomware Attacks Disrupt US Energy Infrastructure and Global Food Supply

Ransomware attacks don't just threaten a company's operational and financial health—the ripple effects can have severe global consequences.

On May 7, 2021, Colonial Pipeline, the largest fuel pipeline in the United States, fell victim to a ransomware attack that caused a complete shutdown of the pipeline for several days. The pipeline shutdown created a widespread fuel shortage, disrupting airline operations and causing gas prices to spike—at one point 87% of gas stations in Washington, D.C. reported being out of fuel. The company paid a ransom of bitcoin worth USD 5 million within hours of discovering the attack, but the decryption tool the attackers provided in return was so slow that operations were not fully restored until over a week later.

On May 30, 2021, JBS S.A., a meat processing company that produces about 20% of the world's meat supply, suffered a ransomware attack that disrupted facilities across the United States and Australia. Prices for meat surged in the days following the attack, as governments urged others in the industry to increase production to mitigate the shortfall caused by the attack. JBS paid the attackers bitcoin worth USD 11 million in an effort to expedite recovery of its systems.

CONTENTS

1. INTRODUCTION

Ransomware attacks have dramatically increased in volume and become more sophisticated in the wake of the COVID-19 pandemic with no sign of slowing down. In 2021, governments and private entities both have reported surges in attacks. As one example, in just the first half of 2021, the United States Financial Crimes Enforcement Network (FinCEN) received USD 590 million in ransomware-related suspicious activity reports, over a 40% increase compared to such reports received in all of 2020. And while companies have become more resilient to such attacks, attackers continue to succeed in wreaking havoc on valuable IT systems and critical data. In a survey conducted in early 2021 of 5,400 IT decision makers employed by a range of organizations across 30 countries, over one-third reported being the target of a ransomware attack—and over half reported that the attackers were successfully able to infect their systems.

In addition to costing companies millions of dollars, ransomware attacks have also become a significant source of regulatory and reputational risk. As privacy and data security increasingly penetrate the global zeitgeist, reports of ransomware attacks have become regular fixtures in international news publications across the globe.

This publication aims to help companies understand and address the risk of a ransomware attack. It provides guidance on how to prevent and prepare for ransomware attacks and what to do if and when a company is the victim of such an attack. It also discusses important legal considerations from different key jurisdictions, and describes how Clifford Chance can help.

Types of Ransomware

"Locker" ransomware attacks directly block access to a device or system. In such an attack, underlying data remains intact.

"Crypto" ransomware attacks encrypt data, rendering it unreadable. Devices or systems remain accessible, but data cannot be processed without a decryption key.

RANSOMWARE: PREVENTION & RESPONSE

CLIFFORD
CHANCE

2. ANATOMY OF AN ATTACK

A ransomware attack combines malicious software (malware) with extortion. Attackers infect devices or systems with malware, demanding payment to restore access. They also often threaten to publish stolen data, to pressure victims to pay ransoms.

Stage 1: Infect

A ransomware attack begins with malware. Attackers exploit vulnerabilities in order to gain access to a device or system. This can be accomplished in a number of different ways. In some cases, attackers can crack weak security defenses and gain direct access to devices or systems, remotely installing malware. Other attackers may exploit system software vulnerabilities to find backdoors into a targeted system.

One means of attack that has become increasingly popular among ransomware groups is spear phishing. Spear phishing involves targeting key employees—such as IT staff—and using social engineering tactics to acquire credentials or access. For example, attackers may send a targeted email purporting to be from a family member attaching a picture file with malicious code. Or they may masquerade as a senior executive needing to "reset" their password due to a security incident. In these instances, attackers will often study their targets in advance to increase the chance of success.

Stage 2: Attack

Once malware has been installed, the actual ransomware attack proceeds. Sometimes malware will stay dormant for a period to avoid detection. Eventually, however, the malware goes to work, crippling the system. In addition, ransomware perpetrators have increasingly begun exfiltrating data prior to issuing an extortion demand, seeking payment as a condition for returning (and not further disseminating) that data.

Stage 3: Extort

Once the device or system becomes fully disrupted, the attackers will make their demands. Most of the time this will be a demand for payment. Typically, these demands seek payment in untraceable cryptocurrency (*e.g.,* Bitcoin).

Stage 4: Spread

Ransomware attackers have become increasingly organized, forming "groups" and conducting repeated attacks over a sustained period of time. Accordingly, ransomware attackers will often look to leverage successful attacks to identify new victims—or continue exploiting existing victims. For example, malware can be designed to lay dormant, before it is activated again months or years later. Attackers can also use their access into one company to attack clients or service providers of that first victim.

3. PREVENTION & PREPARATION

The best way to defend against ransomware is to prevent the attack in the first place, and to be prepared to respond if an attack does occur.

Strong Cybersecurity Measures

Most companies are required by law to have reasonable cybersecurity measures in place to protect personal information. Such measures should help prevent ransomware infections. These measures include:

- Network security (*e.g.,* firewalls, antivirus software, and network traffic monitoring) to prevent and identify intrusions and suspicious activity;
- Software patch management to eliminate software vulnerabilities;
- Remote access security measures (*e.g.,* VPNs, multifactor authentication) to ensure secure work-from-home capability; and
- Segmented networks to limit spread of malware.

Training

Training is critical to preventing attacks. As discussed in Part 2, one of the most common means of introducing malware into a system is through spear phishing. As attackers become more sophisticated, it is more important than ever for companies to train all staff—and in particular key employees such as IT, finance, and human resources personnel—to identify potential attacks. This includes "testing" employees by sending simulated spear phishing emails, and training employees on the measures they should take if they suspect an attack, such as immediately reporting the incident and isolating and segmenting devices suspected to be infected.

Backup & Disaster Recovery

All companies should have an established backup and disaster recovery policy. Where complete system backups are not feasible, backups should be maintained for business-critical data and processes. Backups should be segmented from primary systems to prevent any malware from spreading to such backups.

Incident Response Plans

In addition to disaster recovery, companies should have in place robust incident response plans. The specific elements that should be part of such plans are discussed below, but it is important to understand that such policies and procedures must be well established before an incident occurs. Relevant personnel should be trained on the incident response plan and disaster recovery procedures. Tabletop exercises will help ensure that procedures are effective and efficient, so that staff will be prepared in the event of an actual incident.

Cyberinsurance

As ransomware and other cyber attacks become more prevalent, cyberinsurance has become crucial. Just as with any other insurance policy, however, coverage will vary. For example, not all policies cover actual ransom payments. Understanding these policies in advance will help ensure companies are not caught by surprise if and when a ransomware attack does occur.

4. RESPONDING TO AN ATTACK

Ransomware attacks can happen to even the most well-protected company, so companies must be prepared to quickly mitigate and remediate any damage.

Immediate Response

A robust incident response plan will help companies prioritize key actions they will need to take immediately after discovering a ransomware attack. These include:

- Establishing an internal steering group to oversee incident response;
- Segregating and isolating the malware infection to limit its spread;
- Developing an external communication strategy to control information flow;
- Establishing internal communication protocols to ensure staff are informed;
- Implementing backup and disaster recovery plans to permit business to continue (if appropriate and safe to do so);
- Engaging key external advisors, including legal and forensic advisors;
- Taking care to maximize legal privilege protection over internal communications and (where possible) the work of forensic teams;
- Determining reporting obligations and timelines (including notification to affected individuals, law enforcement and government regulators, and cyber insurers, as appropriate); and
- Examining contractual notification obligations to key counterparties.

Many of these elements can be prepared in advance (*e.g.,* template press releases, approved vendors).

Payment

One of the obvious immediate issues victims of a ransomware attack must consider is whether to pay the ransom. There is no "correct" answer to this question, but companies should consider:

- Whether there are alternatives to payment (*e.g.,* backups);
- Legal ramifications of payment (*e.g.,* sanctions law in the United States, see Part 5); and
- The company's specific reputational concerns.

Notably, research has found that the average cost to a victim of a ransomware attack almost doubles when ransom is paid. And while many companies that pay are able to restore operations and recover their data, payment of a ransom does not excuse regulatory notification obligations, nor does it guarantee that exfiltrated data will not be further disseminated.

Preparing for Litigation

One of the first things companies should do after discovering an attack is consult external counsel, who can advise on steps to take to prepare for litigation or a regulatory investigation.

For example, employees should understand that all communications may be subject to external discovery. Accordingly, communications should be limited as much as possible to factual statements and avoid speculation with regards to cause and consequences.

Any legal advice should be marked as such and distributed sparingly to maintain privilege. In some circumstances external counsel can also establish engagements with third parties to extend privilege protections to their communications.

Spotlight: Attackers Increase Pressure to Pay by Threatening Publication

In recent years, companies have become more sophisticated in their IT security, implementing protective measures against ransomware attacks such as system backups and rollback technology. In response to this increasing resistance, the Maze ransomware group introduced a new extortion technique in 2019—actually exfiltrating data and threatening to publish it. This technique is particularly devastating for companies that possess sensitive personal data for customers, clients, or other third parties. Since this technique was introduced, a number of major ransomware groups have also incorporated the tactic into their playbooks.

RANSOMWARE: PREVENTION & RESPONSE

CLIFFORD
CHANCE

Recovery & Restoration

Whether a company decides to pay ransom or if they rely on backups and third-party decryption solutions, restoration is a process that requires careful planning and execution. Measures IT professionals should implement include:

- Stepwise and segregated eradication and restoration of affected systems;
- Technical safeguards to ensure malware is contained; and
- New systems and credentials, as appropriate.

As ransomware attacks have proliferated, law enforcement and companies have begun to collaborate to respond to the threat. For example, the No More Ransom project has created a repository of resources, including decryption tools for known ransomware variants.

Companies should also consider engaging third-party cybersecurity companies that specialize in ransomware response. These companies provide services ranging from negotiating with attackers to system monitoring and execution of decryption keys.

Investigation & Remediation

While some of the most critical work in responding to a ransomware attack will occur in the days immediately following the incident, much of the work will continue for weeks and months following the attack, in the investigation and remediation phase.

Key considerations for this process include:

- Analyzing exfiltrated data (if any) to determine notification obligations;
- Addressing customer concerns (*e.g.,* by providing identity monitoring services);
- Eliminating the vulnerability (*e.g.,* by enhancing security systems, conducting training) and
- Responding to regulator inquiries.

In addition, once the incident has been fully remediated, the company should review its incident response policies and procedures and address any deficiencies that it observed with regards to these procedures in practice. The investigation should culminate in a written report that details the results of the findings as well as remediation measures the company has put in place.

Spotlight: Attackers Often Go Back to the Same Well

Ransomware response often means overtime and sleepless nights as companies work as quickly as they can to get their systems up and running. So it can be tempting to take a breath after systems have been recovered. However, in some ways this is when a company is most vulnerable.

A global study on ransomware published in June 2021 found that among survey respondents whose companies paid ransoms, 80% said their companies incurred another attack. Almost half of these respondents reported that they believed the subsequent attacks were by the same perpetrators of the original attack.

The UK's National Cyber Security Centre described a worst-case scenario in a blog post in early 2021. In that post, the agency referenced an unnamed company that suffered an attack and paid a ransom of almost GBP 6.5 million. The attackers provided a decryption tool, and the company was able to restore their systems. However, it did not take steps to strengthen their security and address the vulnerability leading to the attack. Two weeks later, the same attacker exploiting the same vulnerability was able to infect the company's system again, forcing the company to make a second ransom payment.

The weeks following an attack are critical to ensuring this doesn't happen. Once systems are restored and business operations are back to normal, a company that has fallen victim to a ransomware attack should prioritize identifying the root cause of the initial attack and hardening its IT security. The only thing worse than suffering an attack is suffering another.

5. LEGAL CONSIDERATIONS IN KEY JURISDICTIONS

While the mechanics of a ransomware attack and the technical prevention methods companies should employ remain the same across jurisdictions, different countries have different regulatory considerations that must be taken into account when responding to a ransomware attack.

Here are some salient examples of juristiction-specific issues.

United States

Paying a ransom is not in and of itself a criminal offense under US law. However, payments to certain parties may violate US sanctions regimes. The US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory in September 2021, updating an earlier advisory issued in October 2020. In the guidance, OFAC once again cautioned companies that ransomware attackers may be sanctioned entities, and reiterated that the US government "strongly discourages" making ransom payments. Parties that assist, sponsor, or provide financial, material, or technological support to sanctioned entities may violate OFAC rules on a strict liability basis—meaning that even if a party had no knowledge that it was engaging in a transaction with a sanctioned person or entity, penalties may apply.

Notably, however, the guidance explained that OFAC has discretion in its response to a violation, ranging from a public penalty to a "non-public response." OFAC went on to discuss the importance of implementing a robust sanctions compliance program as well as having strong cybersecurity and business continuity practices, noting that such measures would be considered a "significant mitigating factor" in any enforcement action taken by OFAC. In a similar vein, under OFAC's Enforcement Guidelines, voluntary self-disclosure of a violation is considered a mitigating factor. The guidance stressed that companies should report ransomware attacks to law enforcement and cooperate during and after an attack, noting that OFAC would consider such reporting and cooperation to be a voluntary self-disclosure, another significant mitigating factor that would make a non-public response more likely.

FinCEN also issued guidance in October 2021 reminding financial institutions of their compliance obligations, including suspicious activity report filing requirements arising from ransomware-related payments. In that guidance, FinCEN demonstrating an increasing sophistication in its ability to identify and track unlawful activity related to cryptocurrency. The takeaway for companies that facilitate cryptocurrency transactions is that they must ensure they have effective detection and monitoring systems in place to identify and prevent suspicious and unlawful transactions. If they let these transactions slip by and FinCEN identifies them, the companies may be penalized for having inadequate processes in place.

In addition, US breach notification laws create a significant compliance burden because they are state-specific. Typically a company's notification obligations will depend, in part, on the state of residence of any individuals whose personal data are compromised during the course of an attack. Thus, if personal data is exfiltrated during a ransomware attack, a time-consuming review of that data may be necessary to determine what notification obligations exist.

United Kingdom

As in the United States, there is no blanket ban on ransom payments in the United Kingdom. However, depending on to whom money is paid and in what circumstances, there are three offences that companies should be aware of:

1. The financing of terrorism: companies should be aware of current counterterrorism requirements under the Terrorism Act 2000 (TA 2000). For instance, under s15(3) and s17 of the TA 2000, a person will be liable if they make a ransomware payment where they know or have reasonable cause to suspect that the funds will or may be used for the purposes of terrorism. Given most cyber attackers act anonymously, it is unlikely, although not impossible, that the payer will be liable under this law.
2. Money laundering: under s328 of the Proceeds of Crime Act 2002, it is an offence to enter into an arrangement that the party knows or suspects facilitates the use or control of criminal property. However, UK courts have deemed that so long as funds are legal until they reach the hands of the cybercriminals, this offense will not bite.
3. Sanctions offences: companies should also be aware of the risk of making payments, whether directly or indirectly, to "designated" individuals or entities listed in the consolidated list of financial sanctions targets prepared by the UK Office of Financial Sanctions Implementation (OFSI), which is a criminal offense in the United Kingdom. Provided reasonable due diligence is conducted, it will not be an offence to make a payment if it can be shown that the payer did not know or have reasonable cause to suspect the funds would be made available, directly or indirectly, to a designated person.

If you have already made a ransom payment, a High Court judgment from 2019 suggests that courts may be willing to help you recover that payment. In *AA v Persons Unknown and Ors, Re Bitcoin*, the judge granted a proprietary injunction over a Bitcoin payment made following a cyber attack to recover the funds from a cryptoasset exchange that housed the receiving account. Injunctive relief may also be granted in respect of stolen information: in mid-2021 in *4 New Square Ltd. v Person or Persons Unknown*, a barristers' chambers in London obtained an injunction requiring hackers to deliver up the information they had obtained from the chambers and/or to delete any information remaining in their possession or control. Whilst criminals are unlikely to comply with injunctions, insurance policies may require proceedings to be started and, should the criminals ever be identified, they could be subject to proceedings for contempt of court. The extent to which courts and authorities in other jurisdictions are prepared to adopt an active role in ransomware cases remains to be seen, although in 2021 the Irish High Court granted an injunction against hackers who had targeted the country's Health Service Executive and had helpfully signed the ransomware notes with the name of their gang.

Companies should also remain alert to the fact that failure to comply with notification obligations often presents a significant and pressing risk following a ransomware attack. Under Article 33 of the GDPR and UK GDPR, organizations must report personal data

RANSOMWARE: PREVENTION & RESPONSE

CLIFFORD
CHANCE

breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach unless the breach is unlikely to result in a risk to individuals' rights and freedoms. If the breach is likely to result in a high risk to individuals' rights and freedoms, organizations must also inform those individuals without undue delay. Further, the UK Information Commissioner's Office (ICO) has warned that businesses should have robust breach detection, investigation, and internal reporting procedures in place to facilitate decision-making as to whether or not notifications are required. Although heavily reduced from the initially headlined amounts, the fines imposed on Marriott International and British Airways in 2020 underscore the importance of deploying adequate data security measures and the value of cooperating with local regulators following any incident. Similarly, the £1.5 million fine imposed on Ticketmaster following an attack that resulted in access being gained via a third-party chat bot on its payment page serves as a reminder of the importance of assessing and mitigating risks associated with third-party providers.

France

The French National Cybersecurity Agency (ANSSI), together with the French Ministry of Justice (FMJ), published a September 2020 a guide on how to anticipate and react to ransomware attacks. Pursuant to this guide, when a company is subject to such an attack, the ANSSI and the FMJ (i) recommend not to pay the ransom and (ii) recommend to file a formal complaint (*plainte*) with the police (or *gendarmerie*) authorities. This complaint must be filed by the company that suffered the ransomware attack and may trigger the opening of an investigation that can lead to the identification of the attackers. This complaint is also often a prerequisite for the payment of damages (for instance, via insurance policies). In France, investigations relating to ransomware attacks and similar cyber attacks are conducted by specialized units within the Paris prosecution service as well as within the police services.

In addition to the notification obligations that may be required under European laws and regulations (as encompassed, where relevant, by French law), in a case where the company suffering a ransomware attack is listed as an operator of "vital importance" (OVI) within the meaning of the French Defense Code, pursuant to the French law on critical infrastructure information protection, entered into effect on 20 December 2013, (as modified) this company must also notify the ANSSI if the ransomware attack occurred on its critical information systems. This notification must include certain information, such as: a detailed explanation of the security incident; a detailed explanation of its consequences and corrective measures; and the technical details to enable the ANSSI to determine the level of risk (*e.g.,* whether the incident qualifies as a "major crisis").

Germany

As in the United States, paying a ransom is not in and of itself a criminal offense in Germany. However, the US sanctions regime may also apply to German companies and therefore the considerations summarized above should be taken into consideration on a case-by-case basis.

Cyber attacks usually trigger various notification requirements. In Germany, notification under Article 33 of the GDPR should generally be made to the data protection authority of the federal state where a company has its registered headquarters. In addition, data subjects need to be informed without undue delay if it is likely that the data breach resulted in a high risk to the rights and freedoms of natural persons (Article 34 GDPR). Further notification requirements may result from contracts between the affected company and its customers or under capital markets law. If the attacked company issues financial instruments the obligation to publish an ad-hoc-statement without undue delay may apply.

Involvement of law enforcement authorities is usually not mandatory. However, law enforcement assistance may be beneficial in connection with potential negotiations with the attackers. Moreover, some cyber insurers may require that the police are informed.

Furthermore, certain companies, such as operators of critical infrastructures, cloud service providers, online marketplaces, and online search engines may fall under the IT Security Act, which contains additional reporting requirements and obligations to disclose information in the event of significant disruptions. In particular, such entities may have to inform the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik – BSI*). Even in the absence of a legal obligation, informing the BSI should be considered as the BSI often has a good overview of ongoing attacks and can help identify the attackers or determine next steps. At the EU level, the European legislator is currently working on amended requirements under the draft NIS2 Directive. This Directive, which still needs to be adopted and then transposed into national laws, provides for the possibility to report cyber attacks to a Computer Security Incident Response team (CSIRT) instead of the BSI. Under the current draft of the Directive a strict timeframe for a first notification of 24 hours would apply.

Finally, some companies might be identified as a "critical entity" by a Member State under the draft EU Directive on the resilience of critical entities. This draft Directive establishes, *inter alia*, reporting requirements and the requirement of business continuity measures as well as the identification of alternative supply chains in the case of certain cyber incidents.. The Directive still needs to be adopted and transposed into national law.

Luxembourg

Paying a ransom is not in and of itself a criminal offense under Luxembourg law but is actively discouraged by regulators. However, the US sanctions regime may also apply to Luxembourg companies and therefore the considerations summarized above should be taken into consideration on a case-by-case basis.

Cyber attacks usually trigger various notification requirements under European laws and regulations, and/or national Luxembourg legislation, including under the GDPR (to the extent that personal data of customers/users/employees is compromised), the Luxembourg law transposing the NIS Directive, and sectorial obligations such as under the law on payment services. In particular, entities operating in the financial sector and under the supervision of Luxembourg's financial sector regulator (CSSF) must notify the latter in case of an external computer attack, as soon as the attack is deemed successful and even if it did not lead to a fraud.

Cyber attacks are subject to criminal sanctions under the Luxembourg Criminal Code, and affected companies may file a complaint with the public prosecutor. The involvement of public enforcement authorities is not mandatory but may be beneficial or required by insurers.

The Computer Incident Response Center Luxembourg (CIRCL)—the Luxembourg computer emergency response team (CERT) for the private sector—recommends reporting the incident and provides for useful guidance in this regard.

China

Paying ransom is not in and of itself a criminal offense in China. However, any payment may incidentally be caught under the PRC Anti-Terrorism Act, if the ransom is paid knowing that it would be used to subsidize or support terrorism activities. So, reporting the case to, and seeking guidance from, judicial or public security authorities is recommended in practice. Moreover, other jurisdictions' sanctions regime may also apply to PRC companies and therefore the relevant sanctions considerations should be taken into consideration on a case-by-case basis.

Cybersecurity incidents trigger notification requirements under the PRC Cybersecurity Law (2016), the PRC Data Security Law (2021) and the PRC Personal Information Protection Law (2021) (the "PIPL"). Depending on the severity of the incident, reporting under the relevant national and regional cybersecurity contingency rules may also be triggered. Certain types of network operators, particularly operators of critical information infrastructures, will have additional reporting obligations, including reporting to the police and industrial regulators.

Notification to affected individuals is also required under the PIPL upon the real or potential occurrence of a cybersecurity incident, unless the data processor is satisfied that the measures taken can effectively prevent the data leakage, comprise or loss from causing damage. However, regulators may still require the data processor to inform affected data subjects if necessary. The specific timeline has not been formulated but based on the latest consultation draft, data processors are expected to inform data subjects within 3 working days upon the occurrence of the incident.

Hong Kong (SAR)

There is currently no law in Hong Kong prohibiting the payment of ransoms. While such payment could potentially be caught under section 25 of the Organized and Serious Crimes Ordinance (since the victim will have reasonable grounds to believe, or even know, that the ransom payment represents the attacker's proceeds of an indictable offense), section 25A provides a defence if the victim notifies an "authorized officer" (*e.g.* the Hong Kong police) of the payment in advance and obtains consent or if the victim notifies an authorized officer as soon as it is reasonable to do so after making the payment. In addition, victims should be mindful of the offenses under the United Nations Sanctions Ordinance (Cap. 537) and the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526), in the unlikely event that a victim suspects or knows that the attacker is a sanctioned person, or is related to any act of production of weapons of mass destruction.

Although there is no cross-sector cybersecurity legislation in Hong Kong, industry-specific notification requirements may be relevant—for example, regulated financial institutions are expected to notify their regulators (the Securities and Futures Commission (SFC), the Hong Kong Monetary Authority, or the Insurance Authority) in the event of a major cyber incident. Given the growing prevalence of remote working in light of COVID-19, in October 2021, the SFC issued a circular suggesting steps to mitigate the risks resulting from IT system attacks (including ransomware attacks) such as developing and maintaining a cybersecurity incident management plan and providing regular training to remote-working staff on the prevention of cyber events.

To the extent that personal data of customers is compromised including in a ransomware attack, the Privacy Commissioner in Hong Kong also encourages companies to self-report and to notify affected customers. In January 2020, the government published a proposal that it be mandatory for data breaches to be notified to the Privacy Commissioner (and relevant data subjects) if they involve a "real risk of significant harm." The precise timetable of this notification requirement becoming law is still uncertain: as of May 2021, the government has indicated that it was considering possible amendments to the law, such as the specified timeframe and mode of notification, and would make reference to laws in other jurisdictions including the GDPR.

RANSOMWARE: PREVENTION & RESPONSE

Singapore

While Singapore law does not specifically criminalize paying a ransom, this is actively discouraged by the Singapore authorities. Aside from there being no guarantee that the compromised files or systems can be recovered even if the ransom were to be paid, certain legislation may potentially be infringed depending on the circumstances

For instance, payments to ransomware attackers may potentially infringe the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA), which criminalizes assisting another person to retain, control, or use the benefits of criminal conduct. Similarly, ransom payments may potentially be caught by the Terrorism (Suppression of Financing) Act, which makes it an offense to provide property or services intending, knowing, or having reasonable grounds to believe that such property or services will be used to facilitate or carry out any terrorist act or to benefit any person facilitating or carrying out such activity. Payments to sanctioned entities may also violate Singapore sanctions laws.

In terms of notification obligations, the CDSA requires a report to be filed with the Commercial Affairs Department where there is knowledge or reasonable grounds to suspect that any property was used or is intended to be used in connection with criminal conduct. Where the ransomware attack affects critical information infrastructure or systems, the Cybersecurity Act and the Monetary Authority of Singapore require owners of such infrastructure or systems to file a report. In addition, where personal data has been compromised, and the scale of the personal data breach is significant and/or is likely to result in significant harm or impact to affected individuals, the Personal Data Protection Commission (PDPC) and affected individuals must be notified.

Australia

Ransom payments are not prohibited under Australian law but are actively discouraged by regulators. The Australian Cyber Security Centre (ACSC) advises against paying ransoms on the view that compromised organizations secure no guarantee that the damage will be reversed and further expose themselves to future attacks by doing so. Similar to the UK, a party who makes a ransomware payment may be liable under Australian terrorism financing, proceeds of crime, money laundering and/or sanctions laws.

Generally, there are no mandatory reporting obligations or penalties for falling victim to cyber attacks except where the victim organization has suffered a notifiable data breach under the Privacy Act 1988 (Cth) (Privacy Act) or is subject to recent amendments to the Security of Critical Infrastructure Act 2018 (SOCI Act) (see below). Organizations may, however, seek to avail themselves of the ACSC's assistance in addressing any such cyber attacks and in doing so, may adopt a prudent approach of reporting such cyber attacks via the ACSC's Report Cyber portal. The ACSC is considered the first port of call in reporting cyber attacks. Reports made to the ACSC will not be considered formal police statements. However, all reports are utilized for assessment and intelligence initiatives by Australian law enforcement authorities and certain reports may be investigated in further detail.

The consequences of a ransomware attack may also be relevant in relation to industry-specific obligations, including additional notification obligations. For example, Australian Financial Service License (AFSL) holders are subject to general obligations under s912A of the Corporations Act 2001 (Cth) to "have available adequate resources (including financial, technological and human resources)" and "risk management systems" which impose the duty to maintain "minimum cybersecurity requirements." Similarly, entities regulated by the Australian Prudential Regulatory Authority (APRA) are subject to the CPS 234 Standard, which aims to ensure that APRA-regulated entities (including authorized deposit-taking institutions such as banks) are resilient against cyber attacks and other information security incidents. AFSL holders and APRA-regulated entities have mandatory breach reporting obligations that could be triggered by any ransomware attack that evidences any deficiency in relation to the aforementioned obligations.

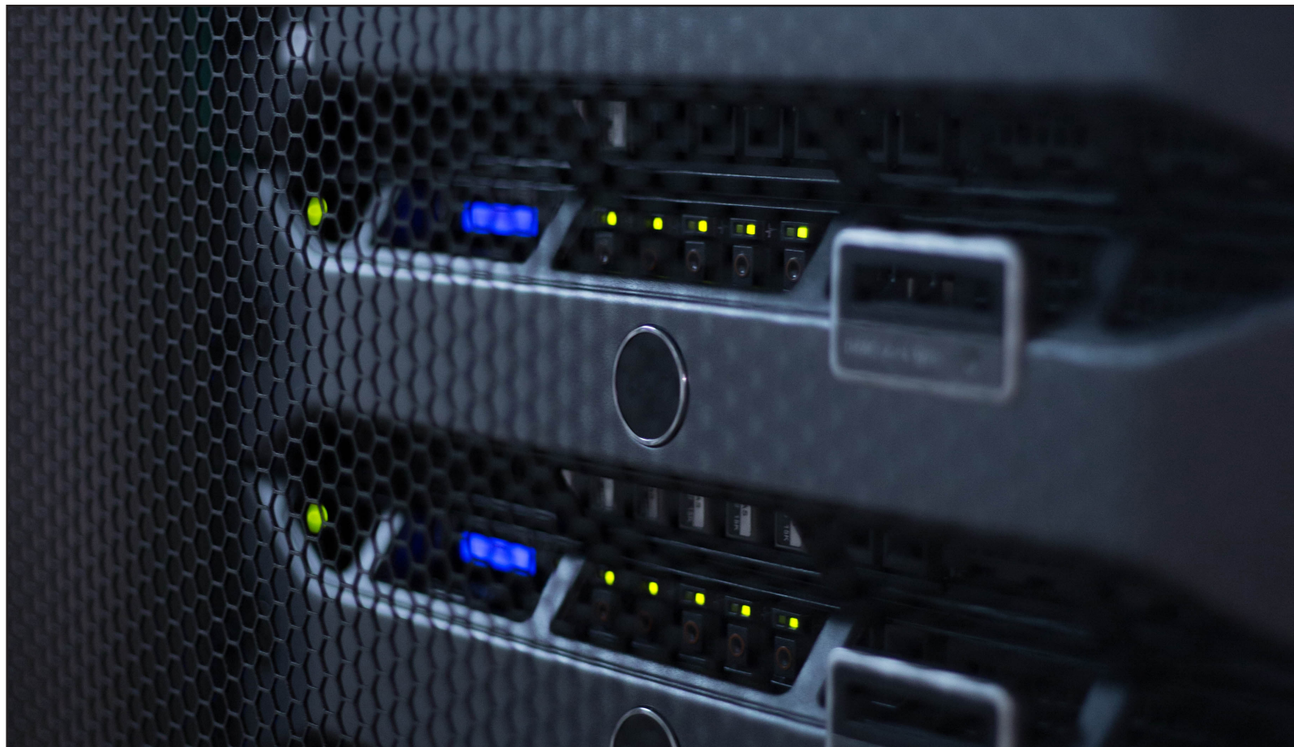
Under the Privacy Act, where there is an eligible data breach as part of a ransomware attack (in particular, where there has been exfiltration of data or unauthorized access to certain types of personal data as part of the attack), there are specific requirements for organizations to notify the affected individuals and the Office of the Australian Information Commissioner (OAIC). An eligible data breach is assessed where: (i) there has been unauthorized access to or disclosure of personal information held by a relevant organization; (ii) that inadvertent access or disclosure can be considered likely to cause serious harm to one or more individuals; and (iii) the organization is unable to mitigate that harm. If an eligible data breach has occurred, the relevant organization must notify the OAIC as soon as practicable as well as each affected individual.

RANSOMWARE: PREVENTION & RESPONSE

CLIFFORD
CHANCE

In response to the increasing instance, severity and profile of ransomware attacks, the Australian Government published its Ransomware Action Plan in October 2021 with three broad objectives: (i) to help organizations and individuals to prepare and prevent to help organizations and individuals respond to and and recover from ransomware attacks; and (iii) to empower government and law enforcement to disrupt and deter those responsible for the attacks.

In November 2021, Australia's parliament passed amendments to the Security of Critical Infrastructure Act 2018 (SOCI Act), which implemented a regime requiring, among other things, mandatory reporting of serious cybersecurity incidents to the ACSC for certain organizations/entities. The amendments also provided emergency government assistance powers to respond to serious cybersecurity incidents (including information gathering directions, directions to act and authority for the Australian Signals Directorate to intervene in response to a cybersecurity incident) and enhanced cybersecurity obligations for "critical infrastructure assets" (which may include assets/infrastructure related to communications, data storage & processing, financial services & markets, water & sewerage, energy, health care & medical, higher education & research, food & grocery, transport, space technology and national defense).



6. HOW CLIFFORD CHANCE CAN HELP

The Clifford Chance privacy and cybersecurity team has extensive experience responding to ransomware and other types of cyber incidents both in the United States and globally.

Deep engagement with the changing regulatory landscape

We regularly assist multinational clients in navigating the complex global privacy and data protection landscape, including regulations such as the California Consumer Privacy Act, the fallout from the Schrems II decision and its impact on cross-border data transfers, the GDPR and NIS Directive, and the New York Department of Financial Service's Cyber Regulation.

A pragmatic, solution-focused approach

Our practice focuses on identifying solutions to our clients' problems, rather than answers to legal questions. We work with clients to assess risk and establish pragmatic approaches where certainty cannot be achieved. We adopt a market-tested, risk-based approach and strive to help clients prioritize and focus on key issues.

A highly experienced team

Our global team regularly advises clients on the full range of issues arising in the context of data privacy and cybersecurity. We have assisted multinational clients to respond to dozens of cyber attacks, and are well versed in key jurisdictions' notification obligations and regulatory expectations. We have handled significant cyber attacks for clients, including a Fortune 100 consumer goods company, a multinational insurance conglomerate, and a global private equity fund. In addition, we have advised numerous clients, including major financial institutions, on their privacy and cybersecurity compliance obligations.

Learn more at **talkingtech.cliffordchance.com**

Connect with us on LinkedIn

Follow us on Instagram

RANSOMWARE: PREVENTION & RESPONSE

CLIFFORD
CHANCE

> **Instead of just repeating the law, they give us a solution to our business challenges.**
>
> **Data Protection & Information law: Chambers & Partners 2020**

> **They are horizon-planning thinkers and they understand market developments in technology.**
>
> **They are on-the-ball, tech friendly lawyers.**
>
> **Chambers & Partners**

GLOBAL CYBERSECURITY CONTACTS

United States

Megan Gordon
Partner
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Daniel Silver
Partner
T: +1 212 878 4919
E: daniel.silver@cliffordchance.com

Ben Berringer
Associate
T: +1 212 878 3372
E: benjamin.berringer@cliffordchance.com

Brian Yin
Associate
T: +1 212 878 4980
E: brian.yin@cliffordchance.com

France

Dessislava Savova
Partner
T: +33 14405 5483
E: dessislava.savova@cliffordchance.com

Grégory Sroussi
Avocat
T: +33 14405 5248
E: gregory.sroussi@cliffordchance.com

Germany

Ines Keitel
Partner
T: +49 697 199 1250
E: ines.keitel@cliffordchance.com

Christian Vogel
Partner
T: +49 175 225 4859
E: christian.vogel@cliffordchance.com

Luxembourg

Dr. Thomas Voland
Partner
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Steve Jacoby
Managing Partner
T: +352 48 50 50 219
E: steve.jacoby@cliffordchance.com

Isabelle Comhaire
Counsel / Senior Legal & Compliance advisor
T: +352 48 50 50 402
E: isabelle.comhaire@cliffordchance.com

Charles-Henri Laevens
Senior Associate
T: +352 48 50 50 485
E: CharlesHenriLaevens@cliffordchance.com

UK

Jonathan Kewley
Partner
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Simon Persoff
Partner
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Kate Scott
Partner
T: +44 20 7006 4442
E: kate.scott@cliffordchance.com

Samantha Ward
Partner
T: +44 20 7006 8546
E: samantha.ward@cliffordchance.com

RANSOMWARE: PREVENTION & RESPONSE

CLIFFORD
CHANCE

Australia

Tim Grave
Partner
T: +61 2 8922 8028
E: tim.grave@cliffordchance.com

China

Ling Ho
Partner
T: +852 2826 3479
E: ling.ho@cliffordchance.com

Kimi Liu
Counsel
T: +86 10 6535 2263
E: kimi.liu@cliffordchance.com

Jessy Cheng
Associate
T: +86 10 6535 4935
E: jessy.cheng@cliffordchance.com

Hong Kong (SAR)

Donna Wacker
Partner
T: +852 2826 3478
E: donna.wacker@cliffordchance.com

William Wong
Consultant
T: +852 2826 3588
E: william.wong@cliffordchance.com

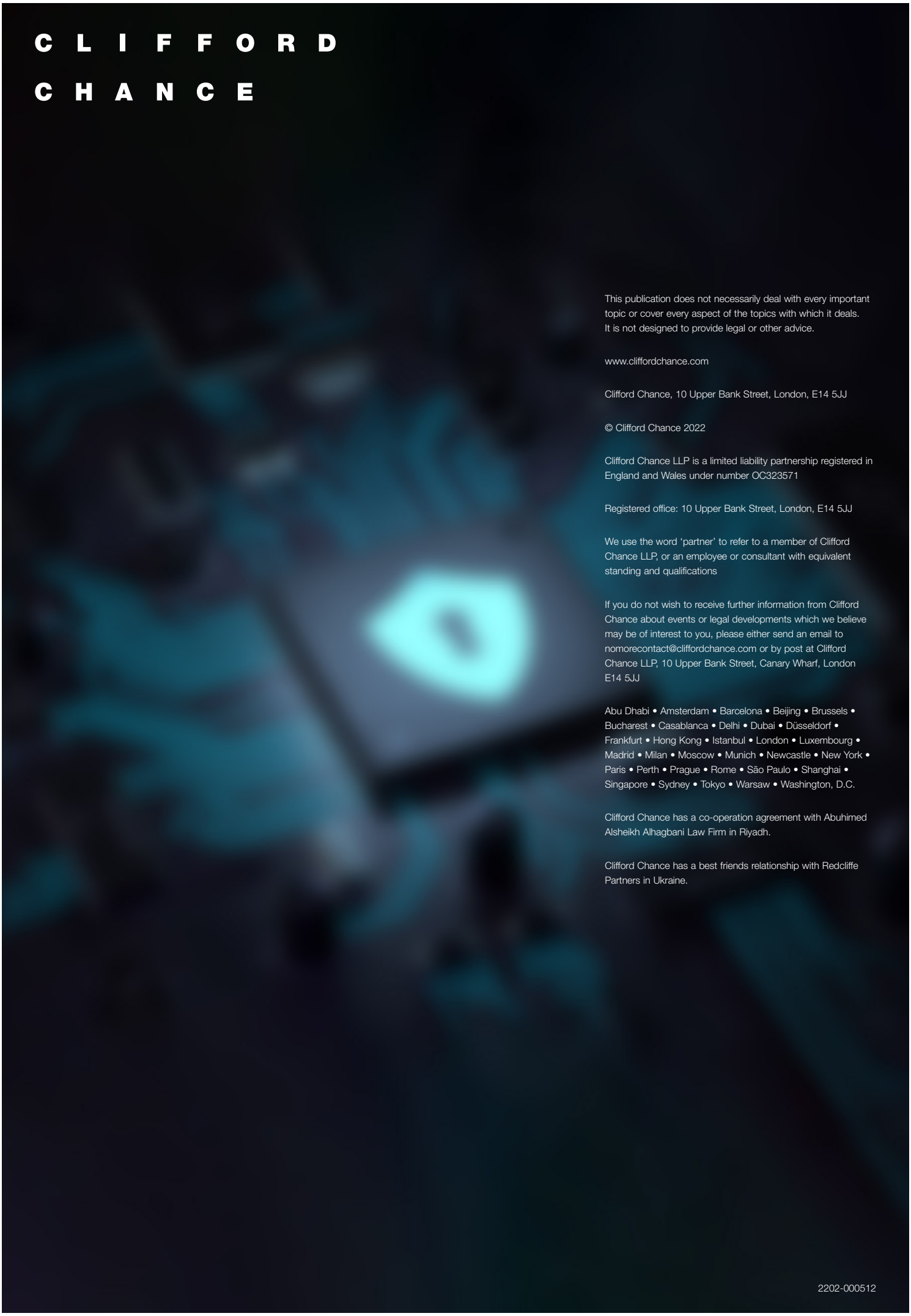
Felicia Cheng
Professional Support Lawyer
T: +852 2826 3526
E: felicia.cheng@cliffordchance.com

Singapore

Kabir Singh
Partner
T: +65 6410 2273
E: kabir.singh@cliffordchance.com

Janice Goh
Partner
T: +65 6661 2021
E: janice.goh@cliffordchance.com

Xide Low
Senior Associate
T: +65 6506 2783
E: xide.low@cliffordchance.com



CLIFFORD
CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2022

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

2202-000512