Chapter Content

1. Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes: The federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, is the primary federal statutory mechanism for prosecuting cybercrime, including hacking. The CFAA provides both criminal and civil penalties, and specifically prohibits: (1) unauthorised access (or exceeding authorised access) to a computer and obtaining national security information (imprisonment up to 10 years); (2) unauthorised access (or exceeding authorised access) to a computer used in interstate or foreign commerce and obtaining information (imprisonment up to one year); (3) unauthorised access to a non-public computer used by the United States government (imprisonment up to one year); (4) knowingly accessing a protected computer without authorisation with the intent to defraud (imprisonment up to five years); (5) damaging a computer intentionally or recklessly (imprisonment up to five years); (6) trafficking in passwords (imprisonment up to one year); (7) transmitting threats of extortion, specifically threats to damage a protected computer and threats to obtain information or compromise the confidentiality of information (imprisonment up to one year); and (8) cyber-extortion related to demands of money or property (imprisonment up to five years). For aggravated offences, criminal penalties can range from 10–20 years of imprisonment. In *Van Buren v. U.S.*, 140 S. Ct. 2667 (2020), the Supreme Court substantially limited the application of the CFAA to insider threats.

Other relevant laws applicable to cybercrimes include the Electronic Communications Protection Act ("ECPA"), which provides protections for communications in storage and in transit. Under the Stored Communications Act ("SCA" Title II of ECPA), 18 U.S.C. § 2702, it is a criminal violation to intentionally access without authorisation (or exceed authorised access) a facility that provides an electronic communications service, including, among others, email service providers or even some employer-provided email. Violations of ECPA are subject to penalties ranging from a fine or up to one year of imprisonment (or both), to up to 10 years for repeat violations for an improper purpose. ECPA also prohibits intentionally intercepting electronic communications in transit under the Wiretap Act (Title I of ECPA), 18 U.S.C. § 2511, with some exceptions for law enforcement, service providers and others (including, potentially, employers). The Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839, the Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1836–1839, and the Wire Fraud statute, 18 U.S.C. § 1343, are further sources of potential criminal and civil penalties against the theft of trade secrets and other valuable intellectual property.

In addition to federal statutes, numerous states have passed statutes prohibiting hacking and other cybercrimes, some of which are broader than the federal statutes. New York, for example, prohibits the knowing use of a computer with the intent to gain access to computer material (computer trespass), N.Y. Penal Law § 156.10, with penalties including imprisonment for up to four years. New York is merely one example; dozens of such state laws exist. Several factors determine which statute applies under conflict of law rules, including the locations of both the alleged act and impacted individuals.

Denial-of-service attacks

Yes: A DOS attack could violate the CFAA, 18 U.S.C. § 1030(a)(5)(A) (intentionally damaging through knowing transmission; the penalty is imprisonment up to 10 years), as well as state computer crime laws.

Phishing

Yes: Among other statutes, phishing could violate the CFAA, 18 U.S.C. § 1030(a)(5)(A) or constitute wire fraud under 18 U.S.C. § 1343, which carries a potential sentence of imprisonment for up to 20 years. Some states have anti-phishing laws such as the California Anti-Phishing Act of 2005.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes: Planting malware would violate the CFAA, 18 U.S.C. § 1030(a)(5)(A) (intentionally damaging through knowing transmission, imprisonment up to 10 years), as well as state computer crime laws.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

18 U.S.C. § 2512 criminalises the manufacture, distribution, possession, and advertising of wiretapping devices, which would include many such tools. Conspiracy to commit an offence is separately subject to criminal sanction. Whether distribution of hacking tools constitutes a crime would depend on whether the actor intended for them to be used for illegal purposes. If there were evidence of criminal intent, a person may be liable for aiding and abetting the violation of the CFAA, 18 U.S.C. § 1030(a)(5)(A), or related computer crime laws. With respect to federal statutes, aiding and abetting is subject to the same sentence as commission of the offence.

Possession or use of hardware, software or other tools used to commit cybercrime

As with distribution, mere possession of hacking tools would be difficult to prosecute in the absence of intent to use them for illegal purposes or related conspiracy. If there were evidence of criminal intent or conspiracy and some overt act taken towards that end, a person may be liable for an attempt to violate the CFAA, 18 U.S.C. § 1030(a)(5)(A), or related computer crime laws. With respect to federal statutes, attempt is subject to the same sentence as commission of the offence.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes: Identity theft could be charged under the federal identity theft statute, 18 U.S.C. § 1028, as well as several analogous state laws.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes: Electronic theft could violate the CFAA, 18 U.S.C. § 1030(a)(2) (obtaining information, without authorisation or exceeding authorisation, imprisonment of up to one year, or five if aggravating factors apply). It may also violate the Economic Espionage Act, 18 U.S.C. §§ 1831–1839, which creates two crimes based on acquiring trade secrets without authorisation, either (1) to benefit a foreign government, or (2) if the theft will create economic benefit for others and will injure the target of the theft. While some courts previously held that obtaining information otherwise available on a computer system in violation of written policies prohibiting such access could violate the CFAA, the Supreme Court found in *Van Buren v. U.S.* that violations of such purpose-based restrictions (i.e., restrictions imposed by contract or company policies) do not themselves constitute violations of the CFAA without other acts that exceed technical restrictions. 141 S. Ct. 1648 (2021).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Yes: Unsolicited penetration testing could violate the CFAA and state laws. If information was obtained from the systems tested, testing could violate 18 U.S.C. § 1030(a)(1) (national security information, imprisonment up to 10 years), (2) (obtaining information, imprisonment up to one year, or five if aggravating factors apply), or (3) (accessing government computers without authorisation, imprisonment up to one year). If the penetration tester causes damage, e.g., by impairing the integrity or availability of a system or data, the action could violate § 18 U.S.C. § 1030(a)(5).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The CFAA, 18 U.S.C. § 1030(a)(2), wire fraud statute, 18 U.S.C. § 2702, and numerous state laws apply to a variety of criminal conduct online.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes: The USA PATRIOT Act amended the CFAA and Access Device Fraud statute, 18 U.S.C. § 1029, to expressly apply them extraterritorially, but complex jurisdictional and venue rules would also need to be considered.

2. Cybersecurity Laws

2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, trade secret protection laws, data breach notification laws, confidentiality laws, and information security laws, among others.

Numerous federal and state laws include cybersecurity requirements. The Federal Trade Commission ("FTC") has been particularly active in this space and interprets its enforcement authority under § 5(a) of the FTC Act, applying to unfair and deceptive practices, to require companies to implement security measures. The FTC has brought numerous enforcement actions against companies it alleges failed to implement reasonable security measures. The U.S. Supreme Court decision in *AMG Capital Management v. FTC* limited the FTC's abilities to seek monetary penalties for potential violations of the FTC Act without first utilising its administrative procedures, although the FTC has continued to seek such penalties in settlements by reference to administrative and other authorities.

Some federal laws, however, are sector-specific or extend only to public companies. Securities law generally prohibits fraud in connection with securities, and the Securities and Exchange Commission ("SEC") has been rigorous in the enforcement of requirements for adequate public disclosures regarding cybersecurity risks and material cybersecurity Incidents for both public companies and regulated financial institutions. Moreover, the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations require "financial institutions" to implement written policies and procedures that are "reasonably designed" to ensure the security and confidentiality of customer records and protect against anticipated threats and unauthorised access and use. Recently, regulators including the FTC and SEC, have adopted or proposed new regulations requiring that covered organisations adopt more specific cybersecurity measures. The Health Insurance Portability and Accountability Act ("HIPAA") includes cybersecurity requirements applicable to protected health information possessed by certain "covered entities" and their "business associates". Computer

crime laws may be used to protect against unlawful hacking, including with respect to the theft of trade secrets.

Many states have also passed laws imposing security requirements. Most of these statutes require "reasonable security". New York's SHIELD Act, for example, requires reasonable security for personal information and specifies measures that may satisfy that standard. The California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, the "CCPA") requires implementation of reasonable security procedures and practices to protect personal information from unauthorised or illegal access, destruction, use, modification, or disclosure and also creates a right of action for Californian residents with statutory penalties of $100 to $750 per consumer and per data breach if the impacted business failed to implement reasonable security procedures. Data protection laws in Connecticut, Colorado, and Virginia that went into operation in 2023 also require "appropriate" or "reasonable" security measures, and Massachusetts regulations have long imposed specific security requirements regarding personal information, including the implementation of a written security programme and encryption of certain data.

All 50 U.S. states plus Washington, D.C. and three federal territories have in place data breach notification laws, and the SEC has recently adopted a final rule requiring public companies to report material cybersecurity Incidents in a Form 8-K within four business days from the date the Incident was determined to be material.

Regarding defensive measures, including a Company's ability to monitor for potential attacks, the Cybersecurity Information Sharing Act ("CISA Law"), 6 U.S.C. § 1501, has two primary impacts. First, it allows companies to monitor network traffic, including taking defensive measures on their own systems. Second, it encourages the sharing of cyber-threat information between companies and with the government.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The CISA Law created the Cybersecurity and Infrastructure Security Agency ("CISA"), a component of the Department of Homeland Security, and the federal agency responsible for protecting critical infrastructure in the United States. CISA coordinates between government and private sector organisations in protecting critical infrastructure and develops and transmits information to private sector entities regarding its expertise in cybersecurity vulnerabilities, Incident response and cybersecurity risk. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), requires "covered entities" – organisations in certain critical infrastructure sectors – to report substantial cybersecurity Incidents to CISA within 72 hours after the organisation reasonably believes the cyber Incident has occurred. Covered entities who are victims of ransomware attacks must make a report within 24 hours of making a ransomware payment. The NPRM was formally published in the Federal Register on April 4, 2024. CISA will publish a final rule by October 2025. The federal government has also issued sector-specific guidance for critical infrastructure operators, and the nuclear, chemical, electrical, government contracting, transportation and other sectors have detailed statutory and regulatory requirements.

2.3 *Security measures*: Are organisations required under Applicable Laws to take specific security measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Generally, yes: U.S. cybersecurity laws exist at both the federal and state levels and vary by commercial sectors. For instance, several federal statutes have data breach notice provisions, but each state has its own data breach law. Many regulators expect regulated companies to have implemented "reasonable" security measures, considering factors such as the sensitivity of the data protected. Considering the proliferation of standards, many companies rely on omnibus cybersecurity frameworks like the NIST Cybersecurity Framework, covering efforts to identify and assess material foreseeable risks (including vendor security), design and implement controls to protect the organisation, monitor for and detect anomalies and realised risks, and respond to and then recover from Incidents.

In addition to general reasonable security requirements, some U.S. state laws or regulations are more prescriptive. For example, the New York Department of Financial Services Cybersecurity ("NYDFS") Regulation includes specific requirements such as annual penetration testing for covered entities. The FTC's revised Safeguards Rule applicable to certain financial institutions specifies measures for the protection of customer information, including encryption and multifactor authentication (or a reasonable equivalent).

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes: All 50 U.S. states, Washington, D.C. and three federal territories have requirements for the reporting of Incidents, and most of these statutes require reporting to state regulators. The nature and scope of the information that must be reported varies by state or territory. For example, California requires the following information in notices to individuals: (1) the name and contact of the reporting person; (2) the types of personal information breached; (3) the date of the breach (or estimated range); (4) whether notification was delayed by a law enforcement investigation; (5) a general description of the Incident (if possible); and (6) toll-free numbers and addresses of major credit reporting agencies.

Timeframes for reporting vary by state or agency, with most requiring notification around the same time that individuals are notified (or sometimes in advance). Vermont requires any notification to its Attorney General ("AG") to be sent within 15 days. Covered financial must report breaches to the NYDFS within 72 hours. At the request of law enforcement agencies, however, some notifications may be delayed.

These state requirements are in addition to federal requirements that are sector-specific. For example, under rules adopted by the SEC, public companies must report material cybersecurity Incidents in a Form 8-K within four business days of making a materiality determination. Public companies must make their materiality determination "without unreasonable delay" following discovery of the Incident. The notification should include information about the nature, scope, timing, and material impact of the Incident. Additionally, public companies must make annual disclosures of material information regarding cybersecurity risk management, strategy, and governance. In February 2022, the SEC issued draft regulations that would require reporting of

"significant adviser" or "significant fund cybersecurity Incidents" within 48 hours of reasonably concluding that an Incident has occurred.

In addition, the Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") requires covered entities and business associates to report certain Incidents involving Protected Health Information ("PHI"). Lastly, Congress passed CIRCIA in March 2022, which will create another reporting regime applicable to certain organisations within critical infrastructure sectors.

Information about cyber threats generally need not be reported, although the federal government encourages participation in Information Sharing and Analysis Centers ("ISACs") or Information Sharing and Analysis Organizations ("ISAOs") where threat intelligence is shared within sector-specific groups of companies. CISA also strongly encourages sharing breach information with it, along with other cyber threat indicators.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

All 50 U.S. states, Washington, D.C. and three federal territories have varying breach notification statutes. These typically require notification to be sent to individuals whose personally identifiable information ("PII"), as defined therein, was acquired or accessed in an Incident. State definitions of PII triggering data breach notification generally apply to electronic data that includes the first name or initial and last name in combination with another identifier, when not encrypted or redacted, such as social security number, driver's licence or identification card number, or account number, or credit card or debit card number. Increasingly, states are also defining PII to include health and biometric information, as well as usernames and passwords that provide access to an online account. Many states also require notice to AGs or other state agencies, depending on the number of individuals impacted. While most states allow for consideration of whether there is a risk of harm to the data subjects, some do not. Timeframes for notification vary by state; however, 30 days is a common standard. Additionally, some sector-specific laws provide notification requirements. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400–414, requires HIPAA-covered entities and business associates to provide notifications in the event of certain Incidents impacting PHI.

2.6 *Responsible authority(ies)*: Please provide contact details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Regulators vary by sector, law, and state, and their details are far too numerous for this publication. The FTC is the principal U.S. federal privacy regulator covering most for-profit businesses not overseen by other regulators, but reporting to the FTC is infrequent. The SEC regulates many financial institutions, and the OCR is primarily responsible for enforcing HIPAA. CISA plays an increasingly significant role in protecting U.S. critical infrastructure, and its role in notification has and will continue to expand. State AGs have broad authority regarding enforcement of cybersecurity. California has a first-in-the-nation regulator, the California Privacy Protection Agency, dedicated to privacy regulation and enforcement. In addition, federal and state regulators in particular sectors, such as insurance, have further enforcement powers.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The United States lacks a unified framework for non-compliance with notice requirements, and penalties depend heavily on the relevant law and regulator, many of which pursue violations as unfair or deceptive trade practices. In addition to regulatory penalties, private plaintiffs may file actions alleging non-compliance with relevant laws. For example, the CCPA provides statutory damages of between $100 and $750 per consumer and per Incident in the event of a data breach caused by the failure to have in place reasonable security measures.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Hundreds of actions have been brought for non-compliance. For instance, Equifax agreed to pay at least $575 million as part of a settlement with the FTC, Consumer Financial Protection Bureau ("CFPB") and 50 U.S. state AGs related to its 2017 data breach allegedly impacting approximately 147 million people. Government authorities alleged that Equifax failed to have reasonable security for the information it collected and stored. Even individual state regulators can extract significant settlements. In 2022, Zoetop Business Company settled with the New York AG for $1.9 million in a data breach allegedly involving 800,000 New York residents; although, millions of account records were potentially compromised worldwide.

3. Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Generally, yes, subject to the CFAA and applicable state law.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

Generally, yes, subject to the CFAA and applicable state law.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

Generally, yes, subject to the CFAA and applicable state law.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber attacks?

Generally, yes: The CISA provides a clear exception to ECPA and creates broad authority to monitor network traffic for "cybersecurity purposes". Employers can generally monitor employee communications if they first provide transparent notice of the monitoring and obtain consent from employees. State torts such as invasion of privacy may also limit an employer's ability to monitor employee communications, but tort claims can be overcome where an employer can show that the employee did not have a reasonable expectation of privacy in the communication. Connecticut, Delaware, and New York have statutes that require notice to employees of such monitoring, and such notices and consents to monitoring should be carefully drafted to ensure compliance.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber attacks?

Yes: Complex and extensive Export Administration Regulations restrict the export of certain strong dual-use encryption technologies; however, licence exceptions may be available for exports.

4. Specific Sectors

4.1 Do legal requirements and/or market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Cybersecurity laws in the United States vary significantly by business sector. There is currently no single U.S. cybersecurity law of general application other than, arguably, restrictions of "unfair" trade practices. Most businesses must comply with sector-specific federal and state laws. Healthcare organisations, for example, generally must comply with HIPAA, and many financial institutions must comply with GLBA. Related state laws impose additional requirements.

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services, health care, or telecommunications)?

In addition to the sectors of critical infrastructure in the United States such as energy, chemical, and transportation, each of which has particular rules, the United States has numerous sector-specific rules applicable to cybersecurity at the federal and state levels. For example, in the financial services sector, organisations must comply with GLBA and its implementing regulations (which vary depending on the organisation's functional regulator). The FTC issued an updated Safeguards Rule applicable to certain financial institutions that went into operation in June 2023, and the SEC has issued its own rules applicable not only to the protection of personal information but also against other cybersecurity risks. The SEC, other regulators, and industry groups, such as the Financial Industry Regulatory Authority ("FINRA") and the National Futures Association ("NFA"), have published cybersecurity guidance that should be carefully reviewed. Red Flag Rules published by regulators require covered firms to adopt written programmes to detect, prevent, and mitigate identity theft. The Fair Credit Reporting Act ("FCRA") and Fair and Accurate Credit Transactions Act ("FACTA") impose requirements with respect to credit reports. The FTC's Disposal Rule, 16 C.F.R. § 682, issued pursuant to FACTA, requires certain practices for the destruction of certain information contained in or derived from a credit report. State regulators sometimes impose very significant further regulations, particularly in New York. A different example would be the Communications Act, as enforced by Federal Communications Commission ("FCC") regulations, which requires telecommunications carriers and providers of Voice over Internet Protocol ("VoIP") services to protect "customer proprietary network information". Substantial fines and penalties can be assessed for failure to ensure adequate protections. Covered entities and business associates under HIPAA are subject to a variety of rules and guidance regarding the protection of certain health data.

5. Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Public company boards of directors and officers owe shareholders fiduciary duties, including the duties of care and loyalty. To fulfil these duties, among other things, boards and officers must exercise appropriate governance over cybersecurity risk by being properly informed regarding the company's cybersecurity risks and the efforts the company has made to address them. Boards must also ensure that investors receive materially accurate disclosures of investment risk.

In an Incident, boards and officers may face scrutiny and, potentially, litigation relating to their cybersecurity oversight. Public companies must publicly report material cybersecurity risks, including material past Incidents. Even if a past Incident is not material, companies should consider it in evaluating disclosures regarding cybersecurity. The SEC has increased its enforcement activity regarding public company disclosures in recent years. For example, in the Yahoo! data breach, individual board members and officers faced a shareholder derivative action alleging they failed to exercise fiduciary duties, failed to ensure that proper security measures were in place, failed to adequately investigate the Incident, and made misleading statements. The allegations were ultimately settled for a reported $29 million. In that same Incident, the SEC issued a $35 million fine. The SEC adopted updated rules regarding breach reporting by public companies in July 2023.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Federal and state laws may impose cybersecurity requirements specific to the entity's functional regulator and the residence of the data subject. For example, the FTC's updated Safeguards Rule, which went into operation in December 2022 and is applicable to certain financial institutions, requires the designation of a "Qualified Individual" responsible for oversight and implementation of the institution's cybersecurity program. Covered financial institutions with more than 5,000 consumers must document an assessment of the institution's cybersecurity risks in writing. Draft SEC regulations applicable to funds and advisers require conducting periodic risk assessments. NYDFS has likewise issued regulations requiring covered financial institutions (including banks and insurance companies) to, among other things, designate a CISO (or equivalent), establish a written Incident response plan, and conduct a periodic risk assessment, annual penetration testing and biannual vulnerability assessments. Massachusetts information security regulations, likewise, require organisations that collect certain Personal Information from Massachusetts residents to implement a comprehensive information security programme that, among other things, identifies and assesses reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of such information. The New York SHIELD Act deems companies compliant with its reasonable security requirement if they implement specified administrative, technical, and physical safeguards, including appointing an employee responsible for coordinating its cybersecurity programme and regularly testing the effectiveness of key controls, systems, and procedures.

6. Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met. Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Organisations that publicly announce Incidents involving a large amount of Personal Information often confront class action litigation from plaintiffs whose information was impacted. These typically involve several theories, including breaches of express or implied contracts, negligence, other common law tort theories, violations of federal or state unfair or deceptive acts or practices statutes, or violations of other state and federal statutes, such as the CCPA. Most prominently, the CCPA creates a data breach right of action for California residents with statutory penalties of $100 to $750 per consumer and per Incident if plaintiffs prove the impacted business failed to implement and maintain reasonable and appropriate security practices.

Contract theories may involve claims of breach of contract where there is a written agreement between the plaintiff and the defendant that contains an express promise of reasonable security measures to protect personal information. Even if no such term is included, many plaintiffs assert implied contract claims, arguing that receipt of their personal information implied a promise to protect it sufficiently. Tort theories involve negligence or other common law theories such as invasion of privacy, bailment, trespass to chattel, misrepresentations, or unjust enrichment. Each of these theories may prove challenging to fit to the data breach context.

Consumer protection theories are often also alleged, claiming that data breach victims committed unfair or deceptive acts or practices. Deception claims are typically premised on an alleged misrepresentation about the security practices of an organisation. Plaintiffs may also allege that a failure to protect information is "unfair", although many courts require substantial injury or widespread and serious consumer harm. Plaintiffs may also allege violations of other statutes such as the federal FCRA or state laws.

In addition to establishing the elements of their claims, plaintiffs filing in federal court must show that they suffered injury-in-fact sufficient to establish standing. Even where an injury alleged is sufficient for standing, it may not be sufficient to state a claim for damages. Some damages theories that plaintiffs attempt to assert, with varying success, include risk of future identity theft, credit-monitoring costs, other costs related to mitigating risks related to an Incident, and overpayment for the products and services associated with the Incident.

While most class actions involve plaintiffs whose information was allegedly compromised, there has been an increase in shareholder derivative and securities fraud actions arising from Incidents as well. In shareholder derivative actions, plaintiffs typically allege that a company's officers and directors breached their fiduciary duties, wasted corporate assets, or committed other mismanagement in failing to ensure that the company maintained what the plaintiffs consider appropriate security. As a preliminary step to any derivative action, plaintiffs must first either ask the board of directors to bring the action and, should the board refuse, prove that its refusal was contrary to the board's reasonable business judgment. Alternatively, they must prove that such a request would be futile. Both theories are difficult to prove.

Plaintiffs may also allege securities fraud. To do so, plaintiffs must allege that the company made materially false or misleading statements, typically regarding the state of its cybersecurity posture, and that the company knew about the falsity of such statements.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

As noted, the public announcement of an Incident will frequently result in class actions and other lawsuits being filed against the impacted organisation. Hundreds of actions have been filed over the years; some recent prominent examples include the following:

- *Altaba* (formerly known as Yahoo!): after announcing an Incident allegedly impacting up to 200 million people, faced consumer class action, shareholder derivative action and securities fraud action, in addition to regulatory investigations, which it ultimately settled.
- *Marriott*: suffered a data breach Incident, resulting in a purported class action, which was certified as a class by the district, only to have the certification overturned on appeal.
- *SolarWinds*: suffered a nation-state intrusion and faced congressional and securities investigations, a securities class action (which was settled), and two shareholder derivative actions, both of which were eventually dismissed, with one decided by the Delaware Supreme Court.

7. Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes: Standalone cyber insurance policies typically cover both third-party liabilities arising from the defence and settlement of Incident-related claims, along with first-party coverage for the policy holder's own losses, which could include investigation costs, legal fees, notification costs, and the costs incurred in providing credit monitoring and identity theft services. Cyber insurance policy forms are typically not standardised and vary significantly from carrier to carrier. Considering the recent increase in ransomware and other cybersecurity Incidents, cyber insurers are increasing rates and demanding more information about companies' security controls. General liability or other policies may, in some instances, cover cyber-related losses, but costs related to Incidents are often excluded.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations specific to cyber insurance, but some states do not allow for insurance against certain violations of law.

7.3 Are organisations allowed to use insurance to pay ransoms?

Yes, but any ransom payment must be screened against applicable sanctions restrictions. U.S. companies are prohibited from making payments to persons listed on the Office of Foreign Asset Control's ("OFAC's") Specifically Designated Nationals and Blocked Persons List, and payment to a sanctioned person may violate such requirements even if the payor is unaware of the sanctions nexus. However, OFAC will consider mitigating factors in determining whether to impose any penalty and, in practice, penalties on entities that have conducted sanctions screens in good faith are rare.

8. Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.

Law enforcement retains numerous powers to investigate Incidents. In addition to standard warrant and subpoena powers, law enforcement may seek records stored by electronic communication services or remote computing services through the SCA, intercept communications in transit through the Wiretap Act or obtain dialling or routing information through the Pen Register statute. The

CLOUD Act authorises law enforcement to access certain information held by a United States-based service provider, even if the data is in another country.

For Incidents involving national security or terrorism, law enforcement may have additional powers. Under the Foreign Intelligence Surveillance Act ("FISA"), the government can obtain information, facilities, or technical assistance from a broad range of entities, subject to extensive targeting and minimisation controls and oversight by a special federal court. National Security Letters ("NSLs") offer an additional investigative tool for limited types of entities.

Federal regulatory authorities such as the FTC, SEC and OCR have powers to investigate Incidents within their respective jurisdictions. State regulators may also investigate Incidents to determine whether any state laws were violated.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under the Communications Assistance for Law Enforcement Act ("CALEA"), law enforcement requires certain telecommunications carriers and manufacturers to build into their systems or services necessary surveillance capabilities to comply with legal requests for information.

No general U.S. laws expressly require organisations to implement backdoors in their IT systems or provide law enforcement authorities with encryption keys. Under the All-Writs Act, some courts in some instances have ordered reasonable assistance, including in one notable case, requiring Apple to assist in circumventing security features, which Apple successfully resisted until it was moot.

9. International Compliance

9.1 How do international compliance regimes impact country-specific cybersecurity rules?

Many larger U.S. firms operate global IT systems. As a result, they generally apply cybersecurity protections that aim for compliance with all applicable global laws. This often results in global companies reporting Incidents within 48 or 72 hours, even if some laws provide 30, 45, or 60 days. Likewise, the exterritorial application of European data protection laws frequently results in U.S. companies accepting EU requirements as a matter of contract.

10. Future Developments

10.1 How do you see cybersecurity restrictions evolving in your jurisdiction?

Prospects for federal privacy or cybersecurity law seem dim. The U.S. Congress has multiple committees with overlapping jurisdiction in this area, and the political divisions within the U.S. have made bi-partisan agreement difficult. Until the U.S. sees one party sweep into power with the White House and both houses of Congress in firm control, we will likely see states continue to experiment with various measures.

10.2 What do you think *should* be the next step for cybersecurity in your jurisdiction?

A uniform federal baseline set of protections, with enhanced protections for some sectors, and pre-emption of state law would provide a much more accessible and comprehensive approach to cybersecurity that would facilitate compliance.

Production Editor's Note

This chapter has been written by a member of ICLG's international panel of experts, who has been exclusively appointed for this task as a leading professional in their field by

, ICLG's publisher. ICLG's in-house editorial team carefully reviews and edits each chapter, updated annually, and audits each one for originality, relevance and style, including anti-plagiarism and AI-detection tools. This chapter was copy-edited by , our in-house editor.