HERBERT SMITH FREEHILLS

CYBER SECURITY QUARTERLY ROUND-UP, NOVEMBER 2018

27 November 2018 | London
Legal Briefings

Cyber security affects all businesses and industries and it is a Board level agenda item. This quarterly eBulletin provides a round-up of best practice, news and legislative developments concerning cyber security in Europe, Asia, Australia and the USA. In this issue, we look at the latest developments on the implementation of the Network and Information Security Directive across Europe, as well as exploring the trend of new data protection legislation globally and the latest in cyber security news and best practice. The changing regulatory landscape is increasingly complex and organisations must ensure that they are prepared.

EUROPE

CONTENT

GUIDE ON NOTIFICATIONS OF OES INCIDENTS

In late July 2018, the NIS Cooperation Group (composed of representatives of the Member States, the European Commission and the European Union Agency for Network and Information Security (**ENISA**)) published non-binding guidance on notifications of an incident under the Network and Information Systems ("**NIS**") Directive (the "**Guidance**").

The Guidance contains an overview of the notification and reporting requirements under NIS where:

- an operator must notify incidents with significant impact, without undue delay, to the competent authority and/or the relevant national Computer Security Incident Response Team ("**CSIRT**");
- if an incident has a significant impact in another European Union ("**EU**") Member State, then the Single Point of Contact ("SPOC") must inform the SPOC in that other Member State; and
- annually, the national competent authorities must send a summary report, to the NIS Cooperation Group, about the notification received from Operators of Essential Services ("**OES**").

The Guidance recommends that an operator immediately alerts the CSIRT of a cybersecurity incident to allow the CSIRT to offer support, assess the incident and inform other interested parties (eg authorities abroad should it have a significant impact across the EU). The operator can then provide follow-up notifications as further information about the cybersecurity incident becomes known.

In relation to whether an incident is "significant", the Guidance states that the definition of significance can differ between the Member States. Whether or not an incident is significant, nationally, depends on the sector, the type of essential service, and national circumstances. The Guidance includes examples of whether an incident is significant or not.

The Guidance also includes details on how operators should notify incidents and notes that multiple notification methods are acceptable as some IT systems may be impaired or unavailable during or in the aftermath of an incident. Technical and security measures including encryption, authentication and confirmation should be taken into account. As each EU Member States implement the NIS Directive notification requirements differently, the Guidance has provided examples.

If there is significant cross-border impact, the Guidance states that the timing and content of the notification between SPOCs will depend on the situation and notes that the SPOC should take care to protect the security and commercial interests of the affected organisation.

For the annual summary reports, the Guidance states that the detailed procedure for the summary reports to the NIS Cooperation Group will be developed and agreed by the NIS Cooperation Group.

EU Member States should consider providing information on cyber security incidents on a voluntary basis even if they are out of the scope of the NIS Directive requirement.

Section 5 of the Guidance provides a template for incident notification that could be used by Member States to develop and implement a national notification process. Details include the nature of the incident, the impact of the incident, contact information, operational information, information sharing and ex-post information sharing. A different template is included in the Guidance for the SPOC to provide the annual summary report to the NIS Cooperation Group. For a more effective analysis of incident notification across the EU, the Guidance states that certain information should be included in incident notifications, such as: descriptive information, statistical information, nature of incidents, category of the root cause of incidents, impact of incidents and whether other Member States were impacted and informed of incidents. The information may be aggregated to avoid identification of operators to protect their interests.

IMPLEMENTATION OF THE NETWORK AND INFORMATION SYSTEMS DIRECTIVE

In July 2018, 17 European Union ("**EU**") countries were written to by the European Commission after failing to meet the 9 May 2018 deadline for implementation of the Network and Information Security ("**NIS**") Directive. The warning letters told the countries to prioritise their adoption of the NIS Directive which requires authorities in EU countries to take steps to ensure the protection of vital economic activities against cyberattacks. The countries that received the warning letter were numerous: Austria, Bulgaria, Belgium, Croatia, Denmark, France, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania and Spain.

Since the warnings were sent, Spain, France, Portugal, Poland, Croatia, Ireland, Hungary and Denmark have transposed the NIS Directive into national law.

ICO PUBLISHES UPDATED GUIDANCE FOR DIGITAL SERVICE PROVIDERS ON THE NETWORK AND INFORMATION SYSTEMS REGULATIONS

In October 2018, the Information Commissioner's Office ("**ICO**") published an updated version of its guidance for Digital Service Providers ("**DSPs**") (the "**Guidance**") under the Network and Information Systems Regulations 2018 ("**NIS**").

The Guidance states that the intention of NIS is to address the threats posed to network and information systems and therefore improve the functioning of the digital economy. Whilst NIS is primarily aimed at improving cybersecurity, it is not in itself a cybersecurity law, nor is its application limited to cyber related incidents. 'Non cyber' causes, such as interruptions to power or natural disasters such as flooding would also impact a DSP and therefore fall within NIS.

The Guidance provides examples of which organisations may be DSPs, what security requirements DSPs are required to undertake, NIS enforcement and incident reporting to the ICO. There is also a helpful section on the nexus between NIS and the General Data Protection Regulation ("**GDPR**").

Although the Guidance is primarily aimed at DSPs it is also helpful for Operators of Essential Services given the role of the ICO as regulator under the GDPR.

NEW CYBER COURT APPROVED FOR LONDON

In July 2018, the Lord Chancellor announced a new flagship court in London specifically designed to fight cybercrime, economic crime and fraud.

The new 18 courtroom legal centre will be built on the site of Fleetbank House and has been developed in partnership with the City of London Corporation and the judiciary and will replace the current civil court, Mayor's and City of London County Court and the City of London Magistrates' Court. It will also include a new City of London police station.

The court is due for completion in 2025, though planning permission and funding arrangements are still to be finalised.

MEPS ANNOUNCE NEW CYBERSECURITY CERTIFICATION

In July 2018, Industry Committee Members of the European Parliament backed a new certification framework for connected devices, along with a stronger role for the EU Cybersecurity Agency.

The new scheme will certify that an information communications technology ("ICT") product, process or service has no known vulnerabilities at the time the certification is released and that it complies with international standards and technical specifications.

The certification will be voluntary and, where appropriate, mandatory and based on three risk-based assurance levels:

1. basic – the ICT appliance or device is protected from the known basic risks of cyber incidents;

2. substantial – known risks of cyber incidents are prevented and there is also the capability to resist cyber-attacks with limited resources; and

3. high – risks of cyber incidents are prevented and the appliance or device is able to resist state-of-the-art cyber-attacks with significant resources.

BANK OF ENGLAND, FINANCIAL CONDUCT AGENCY AND PRUDENTIAL REGULATION AGENCY ANNOUNCE PLANS FOR INCREASED CYBER SCRUTINY

In July 2018, UK regulators published a Discussion Paper (PRA DP01/18, FCA DP18/04) which marks the commencement of a dialogue with the financial services industry on how to advance operational resilience in the sector. As the Discussion Paper explains, the operational resilience of firms and financial markets infrastructure is a priority for regulators, which is viewed as no less important than financial resilience given the potential threat to the regulators' specific objectives and to financial stability.

The Discussion Paper introduces the concept of "impact tolerance" and wants financial services organisations to ensure that they are resilient to a wide variety of threats. It suggests that organisations assume that disruption may occur and that they focus on any vulnerability in their business and operating models. To do this, the Discussion Paper promotes an approach based on preparation, recovery, communication and governance.

Responses closed on 5 October 2018 and will assist the regulatory authorities in developing proposals for consultation.

FCA FINES TESCO BANK £16.4 MILLION FOR FAILURES IN 2016 CYBER ATTACK

In October 2018, the Financial Conduct Agency ("**FCA**") issued a Final Notice to Tesco Personal Finance plc ("**Tesco Bank**") imposing a financial penalty of £16,400,000 following a cyber attack which took place in November 2016.

The Final Notice states that the attackers most likely used an algorithm which generated authentic Tesco Bank debit card numbers and, using those "virtual cards", engaged in thousands of unauthorised debit card transactions. Deficiencies in the design of the debit cards, financial crime controls and in Tesco Bank's Financial Crime Operations Team, led to Tesco Bank's current account holders being vulnerable to an incident that the FCA considered to be largely avoidable and that occurred over 48 hours and allowed the attackers to steal £2.26 million. The attack did not involve the loss or theft of customers' personal data.

The attack started at approximately 02:00 on Saturday 5 November 2016. At 04:00, Tesco Bank's fraud analysis and detection system started to send automatic text messages to Tesco Bank's personal current account holders asking them to call about "suspicious activity" on their accounts. Tesco Bank only became aware of the cyber attack as a result of these calls.

A series of errors then took place, which included Tesco Bank's Financial Crime Operations Team emailing the fraud strategy inbox instead of telephoning the on-call fraud analyst. This resulted in a 21 hour delay in Tesco Bank's Financial Crime Operations Team reaching out to Tesco Bank's Fraud Strategy Team and allowing the attack to continue.

Once the Fraud Strategy Team had been alerted, it was determined that the majority of fraudulent transactions were coming from Brazil using a payment method known as "PoS 91". An attempt was made to put a rule in place to block the PoS 91 transactions. However, Tesco Bank's Fraud Strategy Team did not monitor the rule's operation and it was ineffective as the Fraud Strategy Team had erroneously used the Euro currency code instead of Brazil's country code. The attack was finally halted when Tesco Bank's senior management were made aware and took immediate action to block all online transactions and contactless transactions for debit cards, excluding Chip & Pin, ATM and online banking.

Under the FCA Rules, Principle 2 requires a firm to conduct its business with due skill, care and diligence. The FCA held that Tesco Bank had breached Principle 2 because it failed to exercise due skill, care and diligence to:

- the design and distribution of its debit card;
- configure specific authentication and fraud detection rules;
- take appropriate action to prevent the foreseeable risk of PoS 91 fraud; and
- respond to the cyber attack with sufficient rigour, skill and urgency.

The FCA noted that Tesco Bank cooperated fully with their investigation and agreed to settle at an early stage of the investigation, qualifying them to a 30% (Stage 1) discount. Were it not for this discount, the FCA would have imposed a financial penalty of £23,428,500 on Tesco Bank.

DATA PROTECTION IF THERE'S NO BREXIT DEAL

On 13 September 2018, the UK Government published a series of technical notes setting out the implications in various sectors and areas of a 'no deal' Brexit scenario (i.e. a scenario in which the UK leaves the European Union ("**EU**") without an agreement), including a note specifically covering data protection. The note sets out the actions UK organisations should take to enable the continued flow of personal data between the UK and the EU in the event that the UK leaves the EU in March 2019 with no agreement in place.

Transferring data from the UK to the EU

Even in the event of a 'no deal' scenario, the technical note confirms that there should not be any impact on the transfer of personal data from the UK to the EU and beyond. A combination of the UK Data Protection Act 2018 and the European Union (Withdrawal) Act 2018 would incorporate the GDPR into UK law. As such, the provisions currently found in Chapter V of the General Data Protection Regulation ("**GDPR**"), which prohibit the transfer of personal data outside of the European Economic Area ("**EEA**") without adequate safeguards in place, would remain. UK entities would, therefore, continue to be able to send personal data from the UK

to the EU freely and would continue to need to satisfy an appropriate legal basis to legitimise the transfer of personal data beyond European borders.

The technical note further confirms that, "in recognition of the unprecedented degree of alignment between the UK and EU's data protection regimes, the UK would at the point of exit continue to allow the free flow of personal data from the UK to the EU". However, there is a potential sting in the tail as the technical note provides that the UK will keep this under review – once the UK data protection regime is no longer required to mirror the GDPR, it would in theory be possible for the UK Government to amend the UK rules to provide that, for example, no personal data could be transferred outside of the UK without additional safeguards in place – meaning that this could potentially change in the future.

Transferring data from the EU to the UK

In contrast to the export of personal data from the UK, the import of personal data to the UK from the EU will change on exit. As described above, the GDPR restricts the transfer of personal data outside of the EEA, meaning that in a 'no deal' scenario where the UK is no longer a Member State or part of the EEA, entities wishing to transfer data to the UK will need to satisfy one of the available legal bases for the transfer of personal data.

One such mechanism is a finding of 'adequacy' from the European Commission. The European Commission has stated that if it deems the UK's level of personal data protection essentially equivalent to that of the EU, it will make an adequacy decision allowing the transfer of personal data to the UK without restrictions. However, it has further stated that any decision on adequacy cannot be taken until the UK is a third country (i.e. until after the UK's exit from the EU).

In the absence of an adequacy decision (or in the intervening period of time whilst the European Commission is considering an adequacy decision), organisations in the EU wishing to send personal data to the UK will need to satisfy an alternative legal basis for doing so. The most common such basis is likely to be the use of the so-called Standard Contractual Clauses. These are sets of contractual clauses approved by the European Commission and incorporating various protections for personal data. By entering into the Standard Contractual Clauses, two entities are able to transfer data between each other freely. There are also specific derogations which might apply on a case-by-case basis. For example, the transfer of data is permitted with the explicit consent of the individual data subject. However, in all circumstances, entities will need to proactively consider what action they may need to take to ensure the continued free flow of data.

Further information on how Brexit will impact data protection can be found here.

UK GOVERNMENT LAUNCHES NEW VOLUNTARY CODE OF PRACTICE FOR INTERNET-CONNECTED DEVICES

In October 2018, the UK Government published new measures to assist manufacturers to boost the security of internet-connected devices such as home alarm systems, fridges and toys.

Within the next three years, there is expected to be more than 420 million internet-connected devices in use throughout the UK and poorly secured devices can leave people exposed to security issues and large-scale cyber-attacks.

To deal with this, the Department for Digital, Culture, Media and Sport, working in collaboration with the National Cyber Security Centre, have published plans in a "Secure by Design" review to embed security in the design process rather than seeing it as an afterthought.

The new Code of Practice was developed with industry to improve cyber security, encourage innovation and keep consumers safe. It outlines thirteen guidelines that manufacturers of consumer devices should implement into their product's design to enhance safety. This includes secure storage of personal data; regular software updates to make sure devices are protected against emerging security threats; no default passwords; and making it easier for users to delete their personal data from the product.

Technology companies HP Inc. and Centrica Hive Limited are the first companies to sign up to commit to the code. The Government has also published a mapping document to make it easier for other manufacturers to follow in their footsteps and further work is underway to develop regulations that will strengthen the security of internet-connected consumer products.

USA

CONTENT

US CONSIDERING FEDERAL DATA PRIVACY STANDARDS AND LEGISLATION

The Trump Administration is taking steps to develop federal consumer data privacy standards, which if implemented could replace the country's current patchwork approach to data privacy that relies on different, and in some cases contradictory, state and sector-based regulations.

In September 2018, the US Department of Commerce, via the National Telecommunications and Information Administration ("**NTIA**"), sought stakeholder comments on how the US can advance consumer privacy protection while not stifling innovation. Motivating this consultation was the spate of recent high-profile consumer data breaches, as well as the European Union's General Data Protection Regulation and privacy regulations enacted in some US states which in the Administration's view may impede the flow of information and in turn commerce. Per NTIA's consultation document, "[a] growing number of foreign countries, and some US states, have articulated distinct visions for how to address privacy concerns, leading to a nationally and globally fragmented regulatory landscape. Such fragmentation naturally disincentivises innovation by increasing the regulatory costs for products that require scale. The Administration hopes to articulate a renewed vision, one that reduces fragmentation nationally and increases harmonization and interoperability nationally and globally."

With the goal of "building better privacy protections", NTIA (the federal agency principally responsible for advising the Administration on telecommunications and information policy issues) sought comment on the following outcomes: (i) organisations should be transparent about how they collect, use, share and store users' personal information; (ii) users should be able to exercise control over personal information they provide to organisations; (iii) collection, use, storage and sharing of personal data should be reasonably minimised in a manner proportional to the scope of privacy risks; (iv) organisations should employ security safeguards to protect data they collect, store, use, or share; (v) users should be able to reasonably access and correct personal data they have provided; (vi) organisations should take steps to manage the risk of disclosure or harmful uses of personal data; and (vii) organisations should be accountable for the use of personal data that has been collected, maintained or used by their systems. See NTIA Seeks Comment on New Approach to Consumer Data Privacy, 25 September 2018 (available here). The public consultation closed on 26 October 2018.

In developing this consultation, NTIA worked in parallel with the National Institute of Standards and Technology ("**NIST**") to design a voluntary risk-based privacy framework "to help organizations: better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services." See NIST Statement on Privacy Network, 4 September 2018 (available here).

In parallel with this consultation process, the US Senate conducted a public hearing on 26 September 2018 to examine the privacy policies of top US-based technology firms, review the current state of consumer data privacy, and provide industry with a chance to discuss possible approaches to safeguarding privacy more effectively. In advance of the Senate hearing, several industry players submitted proposals for privacy regulation.

Several industry members testified at the Senate hearing (such as AT&T, Amazon.com, Apple, Google and Twitter, among others). This hearing, along with the pending NTIA consultation, will inform legislative proposals to enact a uniform federal privacy and data breach notification law. It remains to be seen whether any future legislation fares better than prior unsuccessful efforts.

US EASES RULES ON THE DEPLOYMENT OF OFFENSIVE CYBER OPERATIONS

White House officials have confirmed media reports that the Trump Administration reversed a prior US policy that critics say hampered the nation's ability to address increasing cyber threats from state-sponsored actors. While its details are classified, Administration officials indicated that the new cyber policy would give US officials greater flexibility to launch offensive cyber operations.

In 2012, the Obama Administration issued Presidential Policy Directive 20, a classified directive relating to US cyber operations that imposed various guidelines to govern the use of US cyber defence tools. In rescinding that directive, the Trump Administration, per US National Security Advisor John Bolton, has "effectively enable[ed] offensive cyber operations," although the change in strategy, according to Bolton, is not designed to foster first strike cyber operations but rather to "create structures of deterrence" against future cyber-attacks on the US and its allies. See *White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons*, The Wall Street Journal, 20 September 2018.

These disclosures accompanied the White House's release of the "National Cyber Strategy" (available here). This document articulates broad strategic goals rather than specifics, and identifies as cyber priorities the securing and protection of US data networks and critical infrastructure; combatting cybercrime; securing US intellectual property from prying state or industry actors; working with US allies "to impose consequences against malicious cyber actors in response to their activities against [the US] and [its] interests"; countering "the flood of online malign influence and information campaigns and non-state propaganda and disinformation"; and building international cyber capabilities to promote cyber threat information sharing and coordinated multi-national cyber defence efforts.

President Trump lauded the National Cyber Strategy as an "important step" in keeping the US safe from cyber threats. US defence and intelligence officials are now charged with filling in the details of the strategy.

CALIFORNIA ENACTS, AND THEN AMENDS, EXPANSIVE STATE PRIVACY LAW

California, always in the vanguard of US state privacy law, enacted the California Consumer Privacy Act of 2018 ("CCPA"), in June 2018, which expands the rights that California residents have with respect to their personal information.

We previously reported on the CCPA (see here), which under California's law (permitting state residents to propose legislation if they secure enough petition signatures) was headed toward a November 2018 ballot initiative. In advance of that, the state legislature enacted the CCPA, which California Governor Jerry Brown signed into law on 28 June 2018. By enacting the law prior to any ballot initiative, the legislature ensured that it could later amend the legislation (a process that is quite difficult if a law is enacted directly by voters).

As enacted, the CCPA would take effect 1 January 2020, and among other things would:

- provide California residents with the right to request a regulated business to disclose the categories and specific pieces of personal information that it collects about the resident, the purpose underlying the collection (or sale) of that information, and the categories of third parties with whom the resident's information is shared;
- enable residents to request deletion of their personal information;
- authorise residents to opt out of the sale of their personal information by a business;
- prohibit businesses from selling the personal information of residents under age 16 absent parental opt-in;
- permit businesses to offer financial incentives for the collection of personal information; and
- provide residents with a private right of action to enforce the CCPA (in addition to state regulatory enforcement).

The law applies to companies doing business in California that collect the personal information of California residents and either (a) have annual gross revenues in excess of USD 25 million; (b) annually buy, receive, sell or share the personal information of at least 50,000 California residents; or (c) derive at least 50% of annual revenue from selling residents' personal information. In addition, the CCPA applies to the affiliates of such businesses, to the extent they share common branding. As a practical matter, the CCPA will apply to businesses that do any significant online business with California customers, even if those businesses do not have a physical presence in the state.

Barely a month after it was enacted, the California legislature (on 31 August 2018) passed several amendments to CCPA. These included extending to 1 July 2020 the deadline for California regulators to issue CCPA regulations; extending the start of CCPA enforcement to the earlier of 1 July 2020 or six months after the CCPA regulations are published; clarifying that entities already subject to privacy regulation under certain other federal and state statutes, including the federal Gramm-Leach-Bliley Act and California's Financial Information Privacy Act, are exempted from the CCPA; permitting consumers to bring an action to enforce the CCPA without first notifying the state Attorney General (who under the CCPA as enacted could elect to prosecute the alleged violation in lieu of the consumer); and preempting any privacy-related measures that California municipalities might choose to enact (thus ensuring uniform state-wide application of the CCPA). Governor Brown approved these amendments as of 23 September 2018. This may not be the last word on the CCPA, however, and additional legislative adjustments to the statute are certainly possible as stakeholders continue to lobby state lawmakers regarding the scope and breadth of the statute.

California has also waded into Internet-of-Things regulation by passing the Information Privacy: Connected Devices bill (the "**Bill**"), requiring makers of connected devices to include reasonable security features designed to protect the device and any information contained in it from unauthorised access, use or disclosure. The Bill is in response to various security failures involving the increasing number of smart devices in homes. In broad strokes, the legislation provides that if a connected device is equipped with a means for authentication outside a local area network, it should contain either a pre-programmed password unique to each device or a security feature that requires a user to generate a new authentication before first-time access is granted to the device. Default device passwords such as "password" and "admin" are banned.

The Bill gives consumers a cause of action in damages where the failure of an Internet-connected device manufacturer to comply with the legislation causes consumer harm. The Bill also includes provisions requiring device manufacturers to take additional steps to restrict access to their devices by malicious actors, such as by releasing the software security updates and patches throughout the life-cycle of a product. The Bill will take effect 1 January 2020.

US FEDERAL TRADE COMMISSION TO HOLD PUBLIC HEARINGS ON DATA PRIVACY ENFORCEMENT ISSUES

The US Federal Trade Commission ("**FTC**"), arguably the most visible consumer privacy regulator at the federal level, has announced a series of public hearings to address whether changes in the economy, evolving business practices, new technologies and international developments require changes to the agency's data privacy enforcement policies.

The hearings, captioned as the "Competition and Consumer Protection in the 21st Century Hearings," commenced September 2018 and are scheduled to run through early 2019. On the agenda is the entire scope of the FTC's regulatory and enforcement mandate, including competition law and consumer protection. With regard to data privacy, FTC has asked interested parties to address the "intersection between privacy, big data, and competition." FTC is particularly interested in: "(a) data as a dimension of competition, and/or as an impediment to entry into or expansion within a relevant market; (b) competition on privacy and data security attributes (between, for example, social media companies or app developers), and the importance of this competition to consumers and users; (c) whether consumers prefer free/ad-supported products to products offering similar services or capabilities but that are neither free nor ad-supported; (d) the benefits and costs of privacy laws and regulations, including the effect of such regulations on innovation, product offerings, and other dimensions of competition and consumer protection; (e) the benefits and costs of varying state, federal and international privacy laws and regulations, including the conflicts associated with those standards; and (f) competition and consumer protection implications of use and location tracking mechanisms." See US Federal Trade Commission Announces Hearings on Competition and Consumer Protection in the 21st Century (available here).

The FTC has also sought comments with respect to its role in deterring unlawful conduct (which FTC challenges under Section 5 of the FTC Act, prohibiting "unfair and deceptive" acts). Comments are specifically sought on the effectiveness of FTC's current enforcement efforts, and the "identification of any additional tools or authorities the [FTC] may need to adequately deter unfair and deceptive conduct related to privacy and data security."

These hearings and stakeholder input are likely to inform further FTC regulation and enforcement efforts regarding the protection of US consumers' personal and financial data.

ANTHEM'S CLASS ACTION DATA BREACH SETTLEMENT CHALLENGED ON APPEAL

A federal court, in August 2018, approved a US$ 115 million settlement of class actions filed in the wake of the highly publicised 2015 data breach involving the US health insurer Anthem, which resulted in the theft of personal data, including health-related information, of some 79 million health insurance plan members of Anthem or affiliated insurance companies. See *In re Anthem, Inc. Data Breach Litigation*, 15-MD-2617-LHK (N.D. Calif.). That settlement could be in jeopardy, however, as several class members have appealed to overturn the agreement, arguing that it unfairly rewards plaintiffs' attorneys at the expense of individual plaintiffs.

In late 2014 and early 2015, Anthem experienced one of the largest data breaches in US history. Per the court, cyber-attackers gained access to Anthem's database, which contained personally identifying information, such as name, address, birthdate, and Social Security number, and individual health data. After a series of class actions were filed in 2015 and consolidated in California federal court, the parties reached a provisional settlement in June 2017, before the court issued a class certification ruling. In addition to the monetary payment, Anthem agreed to enhance its data security procedures, to provide credit monitoring services (to affected class members who applied for it) for an initial period of two years, to provide a cash alternative to those class members that did not sign up for credit monitoring, and to reimburse members' out-of-pocket losses.

In approving this settlement, the federal court found that it provided "meaningful consideration—a total of $115 million where the class size is approximately 79.15 million. Whether one looks at absolute or per-capita numbers, the size of this fund is significant." This settlement amount, according to the parties, was the largest ever reached in a US data breach class action. However, the court rejected the request of class counsel for attorneys' fees of $37.95 million (or around one-third of the total settlement), finding that having 53 law firms, and over 300 timekeepers, working for the plaintiffs "likely resulted in unnecessarily duplicative or inefficient work." That said, the court still approved a $31 million award to class counsel.

Several class members objected, arguing that the attorneys' fee award was excessive and leaves individual plaintiffs without adequate compensation. As an example, certain members claimed that the credit monitoring offered through the settlement has a retail value of US$ 480, while the cash alternative amounts to less than forty dollars. Briefing on the appeal is set to begin in early 2019, and a decision could issue later that year.

THREE MEMBERS OF INTERNATIONAL CYBERCRIME GROUP "FIN7" ARRESTED FOR ROLE IN ATTACKING OVER 100 US COMPANIES

Three Ukrainian citizens suspected of being part of the Fin7 hacking group were arrested in August 2018 by US police forces. The three men have been accused of using malware to attack more than 120 US companies. Firms in the UK, France and Australia were also targeted.

According to three federal indictments, Dmytro Fedorov, Fedir Hladyr and Andrii Kolpakov are members of a hacking group known as Fin7 (also referred to as Carbanak Group and the Navigator Group). Fin7 members engaged in a sophisticated malware campaign and hacked into thousands of computer systems. This allowed the group to steal millions of customer credit and debit card numbers, which the group then used or sold for profit.

According to the indictments, Fin7, through its dozens of members, launched numerous waves of malicious cyber-attacks on businesses by carefully crafting email messages that appeared legitimate to a business' employee. They also accompanied emails with targeted telephone calls intended to legitimize the email further. Once a file that was attached to the email was opened and activated, Fin7 would use an adapted version of the notorious Carbanak malware amongst other tools to access and steal payment card data for the business' customers.

Fin7 used a front company, Combi Security which was supposedly headquartered in Russia and Israel, to provide a guise of legitimacy and to recruit hackers to join their criminal enterprise.

US ANNOUNCES PUBLICATION OF CYBER-DIGITAL TASK FORCE REPORT

In July 2018, Attorney General Jeff Sessions announced the release of a report produced by the US Attorney General's Cyber Digital Task Force, which was established in February 2018 to answer two questions:

1. How is the Department of Justice responding to global cyber threats?
2. How can federal law enforcement accomplish its mission in this area more effectively?

The report published in July responds to the first question and provides a comprehensive assessment of cyber threats facing the US, defines the challenges posed by cybercrime, describes the Department's work in detecting, deterring, and disrupting threats, as well as how the Department is working with other government departments and with the private sector to respond to cyber incidents.

The report also describes the Department's efforts to protect the 2018 midterm elections and announced a new Department policy that will govern the disclosure of foreign influence operations.

SEC CHARGES FIRM WITH DEFICIENT CYBER SECURITY PROCEDURES

On 26 September 2018, the Securities and Exchange Commission ("**SEC**") announced that Voya Financial Advisors Inc. ("**VFA**"), a broker-dealer and investment adviser based in Des-Moines, has agreed to pay $1 million to settle charges relating to failures in cyber security policies and procedures surrounding a cyber incident where thousands of customer's personal information was compromised.

The SEC charged VFA with violating the Safeguards Rule and the Identity Theft Red Flags Rule, which are designed to protect confidential customer information from identity theft. This is the first time the SEC has commenced enforcement action of the Identity Theft Red Flags Rule.

According to the SEC, the perpetrators of the attack impersonated VFA contractors over six days in 2016 by calling VFA's support line and requesting that the contractors' passwords were reset. The perpetrators then used the new passwords to gain access to the personal information of 5600 VFA customers and used these details to create new online customer profiles to obtain access to account documents for three customers. The SEC found that VFA's failure to terminate the intruders' access was due to weaknesses in their cyber security procedures, some of which had been previously exposed in other fraudulent activity.

VFA has not admitted or denied the SEC's findings, but they have agreed to be censured and pay a $1 million fine. They will also retain an independent consultant to review the company's policies and procedures for compliance with the Safeguards Rule and Identity Theft Red Flags Rule.

ASIA

CONTENT

Further Asia specific continued free flow of data. Asia Technology, Media and Telecoms e-bulletin

INDIA'S NEW DRAFT PERSONAL DATA PROTECTION BILL 2018

On 27 July 2018, an expert committee appointed by the Indian government handed down a draft Personal Data Protection Bill 2018 ("**Draft Bill**"). The Draft Bill follows significant activity involving data privacy law in India, including the Supreme Court's 2017 decision in Puttaswamy which found a data privacy right enshrined by the country's Constitution and the more recent Aadhaar case. If enacted, the Draft Bill would not only create new rights for data subjects, but would also impose important new obligations for data controllers to do with cybersecurity, including the following:

- critical personal data may not be transferred outside of India;
- personal data other than critical personal data may be transferred outside India, but only on the basis of contractual clauses or group schemes approved by the regulator, and to countries or international organisations which have been approved by the government; and
- data controllers must store a copy of all personal data on a data centre located in India.

Following in the footsteps of the General Data Protection Regulation in Europe, the Draft Bill has broad cross-border application. Data processing undertaken by data controllers outside of India is still captured and regulated by the Draft Bill if the data controller is carrying on business in India or where there could be harm to data subjects located in India. Further, a data controller is a data fiduciary, introducing elements of trust into the regulatory mix. This could open data controllers to potential actions based on a breach of fiduciary duty in addition to their statutory obligations.

While the Draft Bill is still subject to change and needs to be passed by Parliament, it is written so as to include provisions which will take effect not more than 12 months of the date of enactment and all provisions must take effect within 30 months of the date of enactment. This means data controllers should now be assessing their obligations under the Draft Bill and if necessary, getting ready to bring their business processes in line with it.

CHINA PLANS NETWORK SECURITY INSPECTIONS FOR THE TELECOMMUNICATIONS AND INTERNET INDUSTRIES

In August 2018, the Ministry of Industry and Information Technology in China issued a notice detailing planned network security inspections for the telecommunication and internet industries in 2018. The key inspection targets are the networks and systems built and operated by telecommunications infrastructure companies, internet companies and organisations involved in the management and service of domain name registrations, all of which are licensed by the telecommunications authorities. The main focus of the inspections is to assess the proper implementation of the laws and regulations (including the Cyber Security Law of the People's Republic of China, the Administrative Measures on Security Protection of Communication Networks, and the Provisions on the Protection of Personal Information of Telecommunications and Internet Users).

CHINA'S BIGGEST DATA THEFT CASE EXPOSES 3 BILLION PIECES OF STOLEN PERSONAL INFORMATION

In the largest case to date involving the theft of personal information, a criminal group illegally obtained over 3 billion pieces of user's personal information by signing marketing advertising system service agreements with several operators in more than ten provinces in China. The companies in the criminal group include a listed company, Beijing Ruizhi Huasheng Technology Corporation. Two companies in the criminal group signed service agreements with operators nationwide. While providing services to such operators, the companies accessed the operators' servers, and embedded into the servers a program which collects personal data from end users of the operators and transfers such personal data to the group's servers outside China. In turn, the group manipulated the users' social accounts and obtained illegal profits. During their investigation, the police found that the case involved almost all domestic internet platforms. Based on their IP addresses, the police found that the conduct was carried out by several companies linked to Beijing Ruizhi Huasheng Technology Corporation and the actual controller of the companies and the criminal group were the same entity. The case is under further investigation. The whole process of the incident highlights the need for effective due diligence regarding the choice of vendor. In the meantime, operators also need to strengthen their supervision and administration on vendor projects.

CYBER SECURITY ATTACK AND DEFENCE COMPETITION HELD FOR THE FINANCIAL INDUSTRY IN CHINA

The People's Bank of China has announced that Alipay has won first prize in the recently held cyber security attack and defence competition. The competition was jointly sponsored by the People's Bank of China, the Ministry of Public Security, the China Banking and Insurance Regulatory Commission, the China Securities Regulatory Commission and other relevant departments. A total of 510 institutions participated. It was held to test the capabilities of various institutions to resist cyber-attacks. A total of 510 institutions participated. The cyber security situation of the financial industry is complicated. The state government is promoting the protection of critical information infrastructure in the financial industry. It is expected that events like this would raise awareness of cyber security in the financial industry, and be a positive influence in cultivating security talents, improving risk prevention and control capabilities, and promoting the development of security technology.

DEVELOPMENT OF NEW CYBERSECURITY STANDARDS FOR AUTONOMOUS VEHICLES IN DUBAI

In July 2018, the Dubai Electronic Security Centre announced that it plans on releasing its own set of security standards for autonomous vehicles.

The standards have been developed to secure self-driving vehicles and ensure that they are fit to use on Dubai's roads. They have been produced in response to cyber threats facing autonomous vehicles and previous failings. The standards include communication security, software security, hardware security and supply chain security.

AUSTRALIA

AUSTRALIA PUBLISHES DRAFT DATA ENCRYPTION LEGISLATION

The Australian Federal Government is looking to provide national security and law enforcement agencies with new powers to access encrypted communications and devices. On 20 September 2018, the *Federal Government introduced the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Cth) (the "**Bill**") into Parliament. The draft Bill:

1. substantially increases the obligations of communications providers operating in Australia to assist law enforcement agencies, through a range of voluntary requests and compulsory orders;

2. introduces computer access warrants, which enable law enforcement agencies investigating Commonwealth offences to search and access content on electronic devices covertly; and

3. strengthens the ability of law enforcement and security agencies to overtly access data through expanded search and seizure warrants.

The Bill would apply to a wide variety of persons participating in the Australian communications market, including carriage service providers, intermediaries, social media platforms, components manufacturers, secure messaging applications and cloud hosting services.

There has been months of national debate relating to the ability of security and law enforcement agencies to force communications providers to build 'backdoors' – systemic security weaknesses – into their products and services to enable access.

The Bill explicitly prohibits a government request that requires a provider to build or implement a new capability to remove electronic protection, such as encryption. However, communications providers may be required to provide access where they already possess the technical capability required to access a user's encrypted communications and devices.

Penalties for each instance of non-compliance include a fine of up to $10 million for a company or $50,000 for an individual.

The Bill is currently before the Parliamentary Joint Committee on Intelligence and Security for inquiry and report who are considering submissions.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

MARK ROBINSON
PARTNER, HEAD OF TMT & DIGITAL, ASIA, SINGAPORE
+65 68689808
Mark.Robinson@hsf.com

JOSEPH FALCONE
PARTNER, NEW YORK
+1 917 542 7805
Joseph.Falcone@hsf.com

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

NICK PANTLIN
PARTNER, HEAD OF TMT & DIGITAL UK & EUROPE, LONDON
+44 20 7466 2570
Nick.Pantlin@hsf.com

MIRIAM EVERETT
PARTNER, LONDON
+44 20 7466 2378
Miriam.Everett@hsf.com

LEGAL NOTICE
