Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

INTERNATIONAL EDITION

OCTOBER 2016

IN THIS ISSUE

Locke Lord LLP

Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy, data protection and cyber risk management. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

OUR AUTHORS:

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Karen L. Booth
Associate
Hartford
860-541-7714
karen.booth@lockelord.com

Charlie Clarence-Smith
Associate
London
+44 (0) 20 7861 9023
cclarence-smith@lockelord.com

Robert Courtneidge
Global Head of Cards & Payments
London
+44 (0) 20 7861 9019
rcourtneidge@lockelord.com

Bart W. Huffman
Partner
Austin
512-305-4746
bhuffman@lockelord.com

John F. Kloecker
Of Counsel
Chicago
312-443-0235
jkloecker@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com

Alan D. Meneghetti
Partner
London
+44 (0) 20 7861 9024
ameneghetti@lockelord.com

Brian L. O'Reilly
Associate
Austin
512-305-4853
boreilly@lockelord.com

Charles M. Salmon
Senior Counsel
Austin
512-305-4722
csalmon@lockelord.com

Philippa Townley
Associate
London
+44 (0) 20 7861 9041
ptownley@lockelord.com

Julia Wheate
Paralegal
London
+44 (0) 20 7811 9283
julia.wheate@lockelord.com

New York DFS Promulgates Cybersecurity Requirements for Financial Services

The New York State Department of Financial Services promulgated proposed cyber security requirements to respond to "the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors." While the DFS stated its appreciation for the fact that many firms have proactively imposed their cybersecurity profile, it determined that certain minimum standards are warranted to ensure the safety and soundness of financial institutions and the protection of customers. Certain elements of the proposed regulation are common to existing requirements found in other jurisdictions and applicable to a broader range of companies. The proposed regulation, however, which is focused on the financial services industry, moves far beyond existing requirements and imposes additional obligations that will be both uncommonly burdensome and potentially risky.

Scope of the Proposed Regulation

The proposed regulation applies to any individual or company operating or required to operate under a "license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law of the State of New York," referred to within the proposed regulation as a "Covered Entity." The proposed regulation is designed to protect all Nonpublic Information, meaning electronic information that is not "Publically Available Information" (as defined by the proposed regulation), as well as the Covered Entity's Information Systems. For this purpose, Information System is defined to include "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination for disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems." Thus, the scope of the requirements far exceeds the more common concepts of Personal Information and the systems on which it resides.

What is required?

Cybersecurity Program and Policy. The proposed regulation requires each Covered Entity to establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems. The cybersecurity program must (1) identify internal and external cyber risks, (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems and Nonpublic Information, (3) detect Cybersecurity Events, (4) respond to Cybersecurity Events, (5) recover from Cybersecurity Events and (6) fulfill regulatory reporting obligations. Each Covered Entity must also adopt a cybersecurity policy, which must address, at a minimum, 14 specific areas, including data governance and classification, access controls and identity management, risk assessment and incident response. On at least an annual basis, the cybersecurity policy must be reviewed by the Covered Entity's board of directors and approved by a senior officer.

CISO. Each Covered Entity is also required to designate a chief information security officer (CISO), which function may be outsourced if certain requirements are met. The CISO is required to report on at least a biennial basis to the board of directors of the Covered Entity. Although other requirements for information security (the Massachusetts data security regulation, for example) impose similar types of requirements, the breadth and specificity of the proposed regulation is, currently, unique.

Assessments and Testing. The cybersecurity program must provide at least quarterly vulnerability assessments and annual penetration testing. Among other requirements, there must also be a risk assessment conducted at least annually and written policies and procedures related to vendors and other third parties that have access to the Information Systems or Nonpublic Information of the Covered Entity.

Encryption. The proposed regulation also imposes specific encryption requirements, requiring the encryption of all Nonpublic Information both in transit and at rest, with a one year grace period for Nonpublic Information in transit and a five year grace period for Nonpublic Information at rest, so long as appropriate alternative compensating controls are implemented. Note that Nonpublic Information is defined much more broadly than the typical definitions of personal information, personally identifiable information, or protected health information used in most encryption requirements.

Incident Response Plan. Each Covered Entity is required to have a written incident response plan to guide its response to and recovery from any Cybersecurity Event. The plan must address seven areas specified in the proposed regulation.

Reporting Requirement. Of particular significance is the requirement to report any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity, or that affects Nonpublic Information, to the DFS superintendent as promptly as possible but in no event later than 72 hours. Given that the definition of Cybersecurity Event includes attempted attacks on data or systems, this notification requirement could impose significant burdens on both covered entities and the DFS itself. We note that while this requirement is triggered only by Cybersecurity Events that have a reasonable likelihood of material of affecting the Covered Entity, or that affects Nonpublic Information, a Covered Entity's determination of effect will presumably be reviewed in hindsight, and Covered Entities may therefore err on the side of over-reporting, or risk being second-guessed in their determination.

Limited Exemption for Small Entities

The proposed regulation provides a limited exemption for Covered Entities with all of the following: fewer than 1,000 customers in each of the last three calendar years, less than $5M dollars gross annual revenue in each of the last three years, and less than $10M dollars in year-end total assets, including assets of all affiliates. Exempted Covered Entities must still comply with the requirements for a cybersecurity program and a cybersecurity policy, limits on access to Information Systems, annual risk assessments, the third party information security requirements, limitations on data retention and the notices to superintendent.

The proposed regulation will be posted for office comment in the New York State Register for 45 days beginning on September 28, 2016. Entities that may be subject to the proposed regulation should carefully analyze its new requirements and, as appropriate, consider providing comments before it becomes effective.

Privacy and Data Breach Concerns in Cloud Computing – Developments in the EU

Over the last few years Europe has increased its focus on cloud computing, and several organizations, working groups and policies have been set up to encourage its expansion and increased usage at the EU level.

For example, the European Cloud Computing Strategy was adopted by the European Commission in September 2012, with an aim of delivering a net gain of 2.5 million new European jobs, and an annual boost of €160 billion to the EU's GDP (around 1%) by 2020, all within the cloud arena. In April 2016, the European Commission announced its plans for the "European Cloud Initiative" which aims to provide an open environment within which 1.7 million European researchers and 70 million professionals in science and technology can store, manage, process and share data (the "European Open Science Cloud"). The estimated investment requirement of the initiative is €6.7 billion.

All of these efforts and initiatives have led to a visible increase in the business of cloud computing and data storage in the EU, including for example:

- in 2015, Apple announced that it will be investing €1.7 billion in new data centres in Europe;
- in 2014 IBM announced the opening of a new cloud data centre in France, and in 2015 IBM announced the openings of its first cloud data centres in Germany and in Italy; and
- cloud storage and sharing tools company Zettabox only stores its customers' data in data centres in Europe (including in Holland, Germany, the UK, Spain, Italy and France).

The 2015 Cloud Security Spotlight study by the Cloud Security Alliance (CSA) found that security is the biggest perceived barrier to cloud adoption, with 9 out of 10 organizations surveyed disclosing that they are concerned about public cloud security. In order to address some of the concerns around cloud computing, the International Information Systems Security Certification Consortium (ISC) and the CSA launched a new certification scheme in April 2015 targeted at cloud security professionals. The new certification scheme, known as "Certified Cloud Security Professional," or "CCSP," is designed as an international standard for professional-level knowledge of the design, implementation and management of cloud environments. CCSP certification will act as an indicator to employers and others that the CCSP-accredited individual is competent in cloud security, and has the knowledge and skills to address security and business issues relating to cloud computing.

This year, on July 6, 2016, the European Parliament adopted the first EU-wide legislation on cybersecurity, the so-called "Network and Information Security Directive" (the NIS Directive). The NIS Directive will apply to providers of "essential services" (for example, electricity/gas suppliers, airports and railways, stock exchanges and healthcare providers) and providers of "digital services" (namely online marketplaces, online search engines and cloud computing service providers). The Directive sets out measures that such providers will need to take in order to ensure the security of their IT systems. The Directive entered into force in August 2016, and EU Member States have 21 months (i.e. by May 2018) to implement the legislation into national law. It is up to each EU Member State to decide which organizations within its jurisdiction fall within the remit of the NIS Directive, which Member States must do within a further 6 months. "Digital service providers" will be subject to the requirements of the NIS Directive if they offer services within the European Union; digital service providers that are established outside of the EU will be required to appoint a representative within an EU Member State and will be required to comply with the national implementing legislation of that Member State.

Whilst improved security is to be welcomed, there is concern that these changes will isolate the EU and form a sort of "cyber-barrier" which will restrict trade. The NIS Directive, for example, may require business to make significant investments to ensure that their security systems are up to standard and to put in place policies and processes for identifying and reporting IT breaches. Such additional costs are likely to be off-putting to larger companies such as Google and Facebook, but may be quite prohibitive to smaller "digital service providers." The European Commission is, as noted above, working on a replacement of the Data Protection Directive with the General Data Protection Regulation (GDPR). Whilst the GDPR does not specifically address cloud computing, there are a number of provisions which will have an impact on the provision and use of cloud services, including in the following key areas:

- **Global reach:** The GDPR contains provisions which have the effect of extending the GDPR's reach to organizations based outside the EU. Article 43(a) has been proposed by the European Parliament to address the issue raised by access requests by public authorities or courts in third countries to personal data stored and processed in the EU. The idea is that a transfer will only be granted by the data protection authority following verification that the transfer complies with the Regulation and it is worth noting that this provision was drafted with particular regard to the growth of cloud computing. The GDPR is intended to apply to data controllers with no EU establishment where they undertake processing related to the offering of goods or services to EU residents, or which monitor individuals resident in the EU, irrespective of whether the processing takes place within the EU.
- **Data processors will also be held responsible:** Under the existing Directive, data controllers (i.e. those persons who determine the purposes for which and the manner in which any personal data are, or are to be, processed) – but not data processors (i.e. those persons that process the personal data on behalf of the data controller) – are responsible for the lawful collection and processing of personal data under their control.
- **Sanctions:** Article 79 of the GDPR, in its current draft, allows national data protection authorities to impose fines of up to €1m or 2% of the worldwide turnover of the breaching entity for personal data breaches. This applies to "anyone who, intentionally or negligently" causes a personal data breach. Cloud computing data breaches have raised concerns about risk of leaks and breaches in cloud storage platforms, particularly when considering the type and volume of data that cloud platforms are able to hold: a single breach could affect hundreds of thousands of individuals.

Whether or not cloud providers will increase their security to give adequate protection to personal data for the moment seems to be a case of "watch this (cyber) space." Companies should continue to monitor for additional developments in the wake of the NIS Directive and in the lead up to GDPR implementation.

Are You Sitting Down? Standing in Privacy Cases After Spokeo

In May of this year, in *Robins v. Spokeo*, the Supreme Court ruled on the important issue of standing for plaintiffs asserting statutory claims for damages in federal court. Some observers thought the decision would guide courts hearing privacy and data breach cases in determining whether a given plaintiff could establish standing to be in federal court with their dispute. In the few months since *Spokeo*, several federal appellate courts have already weighed in, reaching different outcomes when applying the ruling. Based on these early results, a potential split is brewing among the federal circuit courts which could signal a return to the Supreme Court.

In *Braitberg v. Charter Commc'ns, Inc.*, No. 14-1737 (8th Cir. Sept. 8, 2016), the Eighth Circuit addressed an alleged violation of the Cable Communications Policy Act (CCPA), 47 U.S.C. § 551(e), and whether the purported retention of personal information by a cable company met the standard for Article III injury under *Spokeo*. The plaintiff asserted that the defendant cable company retained his address, telephone and Social Security numbers after he cancelled the services. The CCPA requires cable operators to "destroy personally identifiable information [PII] if the information is no longer necessary for the purpose for which it was collected." The plaintiff alleged that this retention of his PII deprived him of the "full value of services" he purchased, and invaded his "federally protected privacy rights." Noting that *Spokeo* requires a "concrete" injury even in the context of a statutory violation, the appellate court concluded that the plaintiff alleged only a "bare procedural violation, divorced from any concrete harm," and affirmed dismissal of his claims. The court noted that there were no allegations that the defendant disclosed the information to a third party or used the information in any other way, and the plaintiff did not identify any "material risk of harm from the retention."

Just days later, the Sixth Circuit reached the opposite result in a data breach case. In *Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386 (6th Cir. Sept. 12, 2016), the Sixth Circuit reversed the dismissal of data breach claims under state law and the Fair Credit Reporting Act. The court held that where the plaintiffs alleged that their personal information had already been stolen and was "in the hands of ill-intentioned criminals," the alleged injury was not speculative. The plaintiffs alleged "substantial risk of harm, coupled with reasonably incurred mitigation costs" from the alleged breach, which was sufficient to establish Article III standing at the pleading stage under *Spokeo*.

Other federal courts have reached divergent results following *Spokeo*. In *Church v. Accretive Health, Inc.*, No. 15-15708 (11th Cir. Jul. 6, 2016), the Eleventh Circuit found standing for a Fair Debt Collection Practices Act claim where the plaintiff alleged that she received a letter that failed to include certain disclosures required by the statute. The court ruled that the plaintiff sufficiently alleged a concrete injury through an "invasion of [her] right to receive the disclosures," because Congress "created a new right" to those disclosures in the statute.

In contrast, the District of Columbia Circuit Court vacated a trial court judgment for statutory violations resulting from point-of-sale zip code collection under *Spokeo*. *Hancock v. Urban Outfitters, Inc.*, No. 14-7047 (D.C. Cir. Jul. 26, 2016). In that case, the court held that the "naked assertion that a zip code was requested and recorded without any concrete consequence" was insufficient and therefore plaintiffs failed to allege an Article III injury. *See also Duqum v. Scotttrade, Inc.*, No. 4:15-CV-1537 (E.D. Mo. Jul. 12, 2016) (threat of harm in data breach claims "too speculative" to provide standing under Article III and *Clapper*).

Spokeo provides only limited guidance as to the standard for Article III standing in actions in which statutory damages are alleged, which is often the situation in data breach and other privacy class actions. As illustrated by the above cases, that lack of specific direction has provided ample fodder for litigants to dispute Article III standing for privacy claims alleging statutory violations and damages. Based on the varying applications by federal courts in the first few months, Spokeo will likely not be the last word from the Supreme Court on this issue.

Coverage and the Duped Employee

What role do cyber and other insurance lines play when losses result from an employee's unwitting participation in spoofed email or password theft schemes? Several recent cases illustrate the evolving coverage implications that arise from the actions of duped employees who, while trying to do their jobs, fall victim to schemes designed to exploit the human element of computer security. Although varied in the specific method of alleged fraud and coverage sought, litigants face a common fact pattern in the above cases: exploitation of human elements – often the weakest link in computer and online security – to induce an insured to take action through electronic means that it would never take if it knew the true source of the request.

A federal court in one recent case sided with the insured in a spoofed email fraud case. *Principle Solutions Group, LLC v. Ironshore Indem., Inc.*, No. 1:15-CV-4130 (N.D. Ga. Aug. 30, 2016). In that case the hacker faked an email from the insured's managing director to its controller. The email referenced a company acquisition and asked that the controller work with a specific attorney to wire funds. Later that morning, the phony attorney sent an email with wiring instructions to a bank in China and called the controller to emphasize that the transaction needed to be completed that day. The controller complied and the fraud was discovered the next day.

The insured sought coverage under its commercial crime policy, which covered losses "directly resulting from a 'fraudulent instruction'" directing a financial institution to transfer funds. On cross-motions for summary judgment, the insurer argued that while the email was an instruction, it did not "directly" result in the loss because of the intervening actions of the insured's employees and the phony attorney. The court disagreed and instead granted summary judgment for the insured, finding the "directly resulting" language to be ambiguous. It concluded that because both parties' interpretations of the policy were reasonable, there was an ambiguity requiring the court to construe the policy in the light most favorable to the insured. *See also Apache v. Great Am. Ins.* Co., No. 4:14-CV-237 (S.D. Tex. Aug. 7, 2015), *appeal pending,* No. 15-20499 (5th Cir. 2016) (granting summary judgment to insured; "[D]espite the human involvement that followed the fraud, the loss still resulted directly from computer fraud, i.e., the email directing Apache to disburse payments to a fraudulent account.").

Real estate closings are also a frequent target. In one pending case, hackers obtained email credentials for the head of a real estate company and sent fraudulent emails from his address to an escrow company requesting withdrawals from the company's account. *Maxum Indem. Co. v. Long Beach Escrow*

Corp., et al., No. 2:16-CV-05907 (C.D. Cal., filed Aug. 8, 2016). The escrow company transferred the funds, which could not be recovered after the fraud was discovered. The plaintiff, a client of the escrow company, alleges in the underlying suit that the escrow company wired funds to the hackers' accounts without communicating directly with the plaintiff by telephone or facsimile, and in doing so failed to follow its own procedures and industry custom and practice. The insurer denied coverage, and seeks a declaration that two exclusions apply: (1) the "funds exclusion" (damages arising out of "commingling, conversion, misappropriation or defalcation of funds"); and (2) the fiduciary duty exclusion (claims arising out of the insured's fiduciary duty, responsibility or obligation). This litigation is ongoing.

Another court denied an insurer's motion to dismiss in a case involving a spoofed email to a title company in a residential real estate sale. *ABL Title Ins. Agency, LLC v. Maxum Indem. Co.,* No. 15-7534 (D.N.J. Jun. 30, 2016). The hacker, using a misleading email address that resembled the seller's attorney email, sent an email indicating that the sellers desired payment by wire transfer. As a result, the title company wired nearly $600,000 to the hacker. The insurer denied coverage under the title company's professional liability policy, and moved to dismiss the title company's lawsuit on grounds that the policy excluded damages arising out of "conversion." The court denied the insurer's motion to dismiss, concluding that it was too early in the proceedings to make a "legal determination that the tort of conversion occurred."

In a pending Texas state court case, the insured alleges that it was the victim of fraudulent emails that impersonated the company's CEO. *Ameriforge Group Inc. v. Fed. Ins. Co.,* No. 4:16-cv-00377 (S.D. Tex., removed from Harris County); *see* Testing the Limits - Cyber Coverage Litigation Update (Locke Lord Feb. 23, 2016). In the spoofed emails, the imposter allegedly instructed an accounting employee to transfer $480,000 in connection with a "strictly confidential financial operation." The imposter cautioned that since the transaction was "very sensitive," the employee should "communicate with me through this email, in order for us not to infringe SEC regulations." Based on those seemingly authentic instructions and a call from a third party "attorney" (also part of the scam), the employee transferred the funds. The insurer has denied coverage on the basis (among others) that the imposter's email does not constitute computer fraud as defined in the policy, because it was not an "unauthorized" introduction of instructions to the computer system, i.e., a hacking event involving unauthorized access or entry to a computer. The litigation is ongoing.

In *Medidata v. Fed. Ins. Co.* No. 1:15-cv-00907 (S.D.N.Y. Mar. 10, 2016), the court denied summary judgment in a case involving forged emails used to deceive finance department employees. The emails caused them to transfer funds to unauthorized overseas accounts. The insurer filed a motion for summary judgment on grounds that there was no unauthorized entry into or manipulation of the insured's computer systems for purposes of the computer fraud policy. Rather, the insurer asserted that the losses were caused by "voluntary transfer" effected by "authorized signatories." Medidata argued in its motion that the emails used an altered sender's code and other data that constituted a fraudulent change to its systems. The court denied both parties' summary judgment motions "without prejudice due to an insufficient record." The order suggests that the court may revisit the motions at a later date following limited expert discovery.

Results for these and similar coverage cases should be watched and will be heavily influenced by the claim-specific facts, the language of the policy (cyber, computer fraud, commercial crime, professional liability or other lines of coverage), and the law of the relevant jurisdiction. But the fact pattern of honest and diligent employees falling victim to trickery by malicious parties to gain access to an insured's computer systems is not going away anytime soon. The increasing frequency of such losses, and the resulting disputes over whether they constitute "computer" or "cyber" losses, should encourage insureds, brokers and insurers to discuss such potential risks and possible insurance components of an insured's overall risk management.

NAIC Revised Draft Insurance Data Security Model Law Continues to Raise Significant Industry Concerns

The National Association of Insurance Commissioners (NAIC) Cybersecurity (EX) Task Force has received significant industry comments regarding its revised draft Insurance Data Security Model Law issued August 17, 2016 (the "Proposed Model Law"). While the revised draft addresses certain concerns voiced by the industry, some comments submitted to the NAIC regarding the revised draft raise significant concerns about key issues such as uniformity and overlapping regulation, onerous breach notification obligations, and the Proposed Model Law's overly broad definition of "personal information."

While the initial draft of the Proposed Model Law would have set "exclusive standards" for data security and breach notification in states adopting the model as drafted, the revised draft complicates this goal, stating that the Proposed Model Law is not to be construed to supersede or alter existing law, except to the extent it is inconsistent. Industry comments stressed the importance of a single, exclusive state law, as uniform among the states as possible, to simplify the existing patchwork of such requirements currently applicable to insurance carriers, producers and others. To this end, certain groups have also recommended that entities subject to HIPAA be excluded from the Proposed Model Law.

A change heavily criticized by the insurance industry removes the harm trigger from the Proposed Model Law's breach notification requirement, thus expanding notification obligations which industry commentators argue are already overly broad, as the definition of "personal information" under the Proposed Model Law potentially extends beyond data elements that could be used for identity theft, and beyond definitions of the term under existing breach notification requirements.

The revised draft of the Proposed Model Law would further shorten the initial draft's extremely tight deadline for notification to state insurance departments. Under the revised draft, notices containing a great deal of information must be provided to the state insurance commissioner within three business days after determining that a breach has occurred – a significantly shorter deadline than those imposed by existing law.

Industry comments also noted approval of a number of the changes made in the revised draft, including elimination of the private cause of action, and removal of privacy notice requirements viewed as confusing and contradictory. In addition, the revised draft clarifies that the Proposed Model Law does not set a single standard for data security programs for all insurance department licensees, but instead, requires that

each licensee's data protection protocols should correspond to the size, complexity and nature of its operations, as well as the sensitivity of the personal information that it collects.

The NAIC has expressed intentions to finalize the Proposed Model Law by the end of the year. Meanwhile, the Texas Department of Insurance issued Commissioner's Bulletin # B-0022-16 of September 15, 2016, which imposes additional requirements for reporting of cybersecurity incidents, and further complicates the existing patchwork of multi-layer state breach notification requirements to which insurers are currently subject.

TalkTalk Loses Appeal Against £1,000 fine at the Information Tribunal

Telecoms service provider TalkTalk has lost an appeal against it for a £1,000 fixed penalty after the Information Commissioner's office (ICO) ruled it had failed to report a personal data breach within the required 24 hours' notice period.

On 17 February 2016, the ICO sent a Notice of Intent to issue a fixed monetary penalty for TalkTalk's failure to notify the Commissioner of a personal data breach within 24 hours of notification from a third party, which they are obliged to do so under the Privacy and Electronic Communications Regulation (PECR).

TalkTalk had been alerted to the data breach upon receiving a detailed account of what had happened by a customer. Having received this information TalkTalk conducted an investigation. TalkTalk says that it was usual practice to notify the Commissioner 24 hours from the conclusion of the investigation and not within 24 hours of the receipt of the complaint. The hack which affected 175,00 customers in 2015 was deemed to have been handled too slowly by the ICO.

Information tribunal judge Angus Hamilton said in his written judgement, "The sole issue in dispute in this case is when TalkTalk could rightly be said to have 'detected' the personal data breach or to have acquired 'sufficient awareness' of the breach."

The Tribunal concluded that TalkTalk had more than 'sufficient awareness' of the breach at the time they received the customer's letter. Companies subject to the ICO's jurisdiction may draw a lesson from the Commissioner's actions and make sure to promptly apprise the ICO of breaches of which they are aware.

FTC: NIST Framework Not Automatic Compliance

In a recent blogpost the Federal Trade Commission made clear that a company does not necessarily meet its information obligations arising from Section 5 of the FTC Act through use of the National Institute of Standards and Technology's (NIST's) Framework for Improving Critical Infrastructure Cybersecurity (Framework). By way of background, Section 5 of the FTC Act prohibits "unfair" and "deceptive" acts by companies dealing with consumers in interstate commerce, and has been used by the FTC for more than a decade to require companies to abide by their promises and to require companies to reasonably secure consumer information. The Framework provides guidance to companies trying to improve their cybersecurity practices through a detailed set of assessment categories within 5 main functions (Identify, Protect, Detect, Respond, Recover).

The FTC addresses the issue as a response to the question "If I comply with the NIST Cybersecurity Framework, am I complying with what the FTC requires?" Within its response the FTC points out that there really is no such thing as compliance with the Framework; rather, the Framework is a practical guide to help companies implement sound security practices. The blogpost states that the Framework and the FTC's approach are "fully consistent," and proceeds to review the FTC's enforcement actions in the information security space over the years. The lessons from those enforcement actions (most of which end up in "voluntary" consent decrees) are sometimes referred to as the "common law" of FTC enforcement in the area of information security.

About a year ago, the FTC has provided similar guidance in its "Start with Security: A Guide for Business." The Guide for Business is also a helpful introductory document for companies seeking to get their arms around basic information security issues. It summarizes the FTC's views on information security into the following points:

- build information security into decision making;
- control access to data sensibly;
- require secure passwords and authentication;
- store sensitive information securely and protect it during transmission;
- segment your network and monitor who's trying to get in and out;
- secure remote access to your network;
- make sure your service providers implement reasonable security measures;
- put procedures in place to keep your security current and address vulnerabilities that may arise; and
- secure paper, physical media, and devices.

Companies who are sharpening their information security practices should take special note of the highlights from FTC publications such as the recent blogpost and the Start with Security publication. The Framework is a valuable tool in connection with exercise, as the blogpost points out.

U.S. Department of Transportation Checklist for Self-Driving Cars

Some of 2016's most exciting technological advances have involved the use of—and planning for the use of—self driving cars. Earlier this month, the U.S. Department of Transportation released their Federal Automated Vehicles Policy and accompanying Fact Sheet: Federal Automated Vehicles which are intended to encourage a "proactive safety approach that will bring lifesaving technologies to the roads safely while providing innovators the space they need to develop new solutions."

The Policy sets forth a forward-looking proposed regulatory framework for dealing with issues relating to self-driving cars through several mechanisms, including a 15-point "Safety Assessment" for the safe design, development, testing and deployment of automated vehicles, a Model State Policy and discussions of current and "modern" (potentially new) regulatory tools. The Safety Assessment aspect of the Policy reflects significant concern about privacy and cybersecurity, and balances that concern with a keen understanding of the unique

nature of this new industry. Without overly specific guidance as to how information should be treated or used, the Policy aims to allow "government, industry and the public to increase their learning and understanding as technology evolves, while protecting legitimate privacy and competitive interests." Examples found in the Policy of the desire for a collaborative partnership to advance both public and private interests include recommendations that:

- manufactures voluntarily report on their compliance with the Policy, including with respect to privacy considerations;
- manufacturers develop processes and standards for collection and use of data (including crash data and other information that may be useful in enhancing safety);
- generally, only de-identified data collected via the operation of self-driving cars should be shared with third parties;
- manufacturers adopt privacy policies and practices that ensure several core principles with respect to treatment of personal information (transparency, choice, respect for context, minimization and de-identification and retention, data security, integrity and access and accountability); and
- vehicle cybersecurity issues be addressed using a "a systems-engineering approach to minimize risks to safety, including those due to cybersecurity threats and vulnerabilities."

The Policy reflects a significant effort on behalf of the government to weight its duty to ensure the safety of the traveling public alongside the development of emerging technologies that will present new opportunities and challenges with respect to collection, use and sharing of information. Manufacturers, individuals and other users of self-driving cars should account for the Policy in developing their own practices, and keep an eye on further developments in the area.

A System of Voluntary Self-Identification in the World of Virtual Currencies

On 5th July 2016, the European Commission (**the "Commission"**) published a proposal for a Directive amending the Fourth Money Laundering Directive (**"Proposed Directive"**), which sets out, amongst other things, to bring into scope currently unregulated virtual currency (**VC**) exchange platforms and custodian wallet providers. These entities would now have to carry out customer due diligence (**CDD**) measures and report suspicious transactions to the relevant Member States' Financial Intelligence Units (**FIUs**).

This is intended to tackle the anonymity associated with VC and to make the information on the identity of users easily available to FIUs, although it is admitted that in itself this measure does not eliminate anonymity as VC can be traded without these intermediaries.

Our view is that a system of voluntary self-identification of VC users could be a ground-breaking development in the world of VC. Is it something that is coming further down the line or maybe a significant opportunity is being missed here?

Allowing self-identification of VC users is not immediately apparent as one of the measures which have been deliberated by the Commission as part of the changes concerning VC. The Explanatory Memorandum to the Proposed Directive only alludes that out of six options considered, the option maintained includes "*allowing more time to consider options as regards a system of voluntary self-identification of virtual currency users.*" This option, therefore, has not made it into the text of the Proposed Directive, apart from a reference in Recital (7), which states "*the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed*".

The Commission's impact assessment sheds more light into what options were considered. The option of requiring mandatory registration of users was ruled out. The voluntary registration alternative included VC users self-identifying themselves to national authorities or to an international body such as the EBA (with acknowledged cost-efficiencies for the latter option). It has been put forward that this would enable FIUs to rapidly verify the identities of registered users[1]. It also has been correctly acknowledged that this could go a long way of "weeding out" criminals who would be unlikely to register.

Had this registration proposal made its way though, it could have provided a perfect solution for VC exchanges or custodian wallet providers for verifying the identity of its users. You can imagine a world where such a centrally-operated VC user register could operate akin to electronic identity verification databases, for example in the UK, where the information collected about the user is compared against the information held in databases for satisfying know-your-customer (KYC) obligations.

But perhaps this is wishful thinking.

Cost and complicated organisational implications provided an immediate barrier. Furthermore, in practice, would a national authority or the EBA be able to carry out this job? It is also not likely to be directly within the remit of the services to be provided by any such authority, without an explicit legislative mandate to make a register accessible to companies for CDD purposes (as, for example, has now been done in respect of company and trust ultimate beneficial ownership information registers).

Also, the effectiveness of any such register (to the FIUs as much as VC exchanges or wallet providers) is also only as good as the checks on the information submitted. For example, it was not clear if it would be part of the registration process to verify (let alone if it was to be to a standard that could be relied upon for CDD purposes) the identity of VC users. The impact analysis hints that the register was considered to only hold two data fields: the identity of the user and VC addresses[2]. If the identity of the users is not verified at this point, the whole exercise seems rather pointless as VC users could use bogus identities.

Although it seems that the voluntary registration was close to making it into the proposal, as it was part of the "preferred package" according to the Commission's Impact Assessment[3], perhaps it is not surprising it has not made it through to the Proposed Directive given that, alongside the proposed date of its transposition (December, 2016) there is very little time to resolve any questions, let alone determine how to implement the infrastructure for such registration.

So where does this leave the VC exchanges and custodian wallet providers?

[1] Commission, 'Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC' SWD(2016) 223 final, para. 5.3.2.1.
[2] *Id.*, para. 6.3.2.1.1.
[3] *Id.*, para. 6.3.2.4

Under the proposal they will have to perform CDD on their users, without the comfort of checking any register. The Proposed Directive also does not provide a comprehensive regulatory framework of VC exchanges/wallet providers as they will not be regulated in the same way as other payment service providers.

Without passporting, VC exchanges and custodian wallet providers will possibly have to get licensed or register in every single EU country they intend to provide VC-related services in and, given the nature of VC and ease of transfers, it is not likely to be immediately clear which competent authority they are now answerable to. Whilst the Proposed Directive allows flexibility in the methods employed to verify the identity of VC users, those who know anything about operating across Europe will know that differences in national implementation of directives often hinder successful replication and economies of uniform systems and controls around areas such as know-your-customer.

So could a trusted third party come forward to take on a voluntary registration outside the Proposed Directive?

This is clearly an opportunity for a global or at least EU trusted third party to take on and offer a real solution to I.D. for VC users. The key elements required, initially, are a secure trusted platform to hold the data and run the register, a fully verifiable and auditable KYC information gathering and verifying system, and a reputation both in technology, KYC and law that enables both the VC users and the regulators to accept it. So how could this voluntary register (VR) work and how could it be made commercially viable? Firstly, it would need to be easily accessible to all VC users in a viral way such that if you register you can also view your counterparty to see if they are also registered. If they are also registered you know they are trusted. You can also, with the counterparty's authority, get confirmation from the VR that they are who they say they are and that they have had their I.D. registered and verified. This also gives the opportunity for the VR to store different levels of I.D. verification to give different levels of clearance. In addition, in a similar way to Amazon and Uber, after each transaction each of the VC users could rate their counterparty and the cumulative rating could also be held on the VR for registered VC users to view. In this way, over time, the VR could become a very powerful tool in the VC community giving VC users a lot more confidence in the VC world and in turn really giving credibility and legitimacy to VC's.

Conclusion

What is clear is that any system of voluntary self-identification by VC users is still a long way off working in practice and at any rate not in a way that could be used by VC exchanges or custodian wallet providers as a meaningful source of information for know-your-customer purposes in time for Proposed Directive's changes coming into force.