Breach Reading 3.0

Cybersecurity & Data Privacy Review

2018

Debevoise & Plimpton

Breach Reading 3.0:

Cybersecurity & Data Privacy Review

Contents

U.S. DATA PRIVACY

GLOBAL SURVEY

UK

China

Russia

Introduction

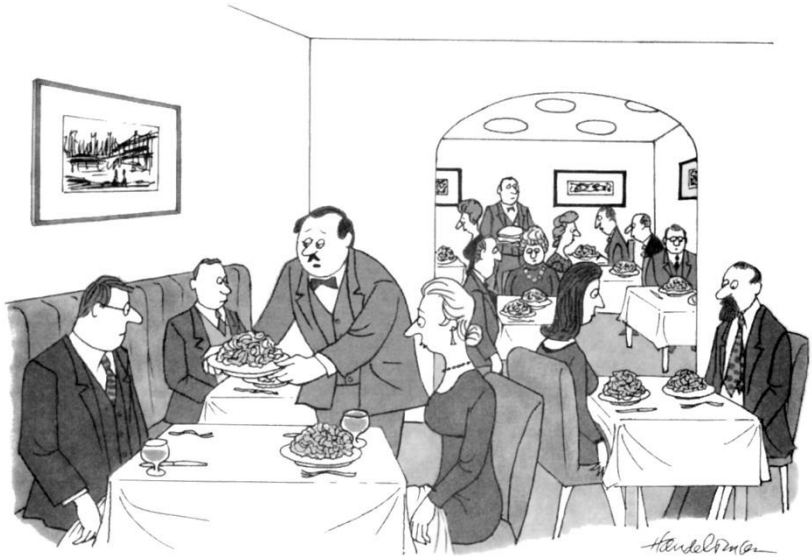
Welcome to Breach Reading 3.0—a compilation of our thoughts on the latest threats, legal obligations and opportunities regarding cybersecurity and data privacy. We hope these thoughts will be useful to in-house counsel, executives, and directors looking to understand how the law now expects companies to manage cyber and privacy risk. The past year has brought new cyber threat vectors, like the sharp rise in enterprise-level ransomware attacks, along with new privacy requirements from a host of sources. Most prominently, Europe's General Data Protection Regulation finally took effect, and California suddenly passed its GDPR-like Consumer Privacy Protection Act.

This third edition of Breach Reading includes both original articles and refreshed versions of the Debevoise Updates that we send from time to time throughout the year. If you'd like to receive those updates, or share any other feedback, please email us at breachreading@debevoise.com, or visit us at www.debevoisedata.com.

Enjoy Breach Reading 3.0, and enjoy your summer.

LUKE DEMBOSKY
JEREMY FEIGELSON
JIM PASTORE
JANE SHVETS

Ransomware



"Sorry, folks—it's not what you ordered, but everyone is getting fettuccine until we fix the computer."

In the past three years, ransomware has become an issue of significant concern for companies across the globe. Ransomware poses a significant operational risk: malicious software encrypts computer files, meaning that companies can lose access to their email and servers in a matter of minutes. The ransom demanded for the keys to decrypt files usually has to be paid in a hard-to-track digital currency such as Bitcoin—which few companies have ready access to, especially in the amounts required to decrypt a large number of systems. Recent ransomware targets have included a wide

range of corporations, hospitals and government agencies, including the French car manufacturer Renault SA, U.S. delivery company FedEx, the city government of Atlanta, Britain's public health system, and the Russian Ministry of Interior. In this section, we provide several updates on ransomware attacks and how to manage this particularly serious cybersecurity risk.

How Ransomware Works. Ransomware often starts with an unsolicited phishing email designed to trick the user into opening an attachment or visiting a webpage. The ransomware software then exploits flaws in the computer's operating system to encrypt important files on the system and demands a payment using a digital currency, typically Bitcoin.

Ransomware Trends. More recent, advanced forms of ransomware have leveraged automated file-sharing to spread much more rapidly both within and among organizations than phishing alone can accomplish. Virtually all types of ransomware will replicate and spread as far within the network as possible. Significant trends in ransomware include an increased focus on selecting high-value corporate targets (akin to a spear-phishing version of ransomware) and a corresponding significant increase in price. Early ransomware demands were in the low hundreds of dollars, typically associated with indiscriminate distribution of the malicious code such that many individual citizens and small businesses were victimized. Recently, the trend is for attackers to devote significant time and effort to gain access to encrypt the files of large businesses and to demand ransoms that range from tens of thousands of dollars to payments in the low millions.

Recent Ransomware Attacks. Two of the most significant ransomware attacks receiving world-wide media attention were

WannaCry and NotPetya. The WannaCry ransomware attack began on May 12, 2017. WannaCry targeted computers running Windows, and encrypted data and then demanded ransom payments in Bitcoin. According to Cyence, a cyber-risk modeling firm, this attack led to companies paying around $10 million in ransom to restore access to their encrypted files. WannaCry affected hundreds of thousands of machines in more than 150 countries, with Russia, Ukraine, and India among the most widely affected.[1]

In Brazil, Brazil's Foreign Ministry, and a dozen Brazilian court systems were affected and had to disconnect computers as a precautionary measure. In England and Scotland, one in five National Health Services hospitals were affected and up to 70,000 devices including computers, MRI scanners, blood-storage refrigerator were affected. The French carmaker Renault halted production in both Slovenia and in France. Spain's Telefónica, FedEx, and the Deutsche Bahn were also all impacted.[2]

About a month later, on June 27, 2017, the NotPetya attack began ("NotPetya" being the rather inartful name given by security researchers to distinguish this malicious code from a similar code called Petya that was unleashed in 2016). NotPetya forced Ukraine's Chemobyl Nuclear Power Plant to go offline, and affected systems at Maersk and DHL, among many others. Maersk, one of the largest container shipping and supply vessel operators, reported about $200

---

1 Deloitte, *Prepare for Ransomware: WannaCry, Petya, and Beyond*, WALL ST. J. (Nov. 3, 2017), http://deloitte.wsj.com/cio/2017/11/03/prepare-for-ransomware-wannacry-petya-and-beyond/.

2 The Associated Press, *The Latest: Researcher Who Helped Halt Cyberattack Applauded*, U.S. NEWS (May 13, 2017), https://www.usnews.com/news/business/articles/2017-05-13/the-latest-turkey-among-countries-hit-in-cyberattack.

to $300 million in lost revenue as a result of the Petya ransomware attack.[3] DLA Piper, a prominent law firm, was also victimized by this attack, disrupting the firm's global network operations within minutes.[4]

Significantly, NotPetya turned out to be pseudo-ransomware. Despite presenting victims with a typical ransom demand screen, the malicious code was designed simply to destroy files, and no payment mechanism was ever set up. The CIA has stated publicly that NotPetya began as a nation-state attack on Ukrainian facilities that spread far beyond the original targets.[5]

Most recently, on March 22, 2018, the City of Atlanta was hacked by the SamSam hacking crew, which spread ransomware across a huge number of city systems. SamSam is known for picking targets that are more likely to pay high ransoms—over $50,000.[6] It has been reported that the hackers sought $51,000 in Bitcoin to decrypt

---

[3] Jordan Novet, *Shipping Company Maersk says June cyberattack could cost up to $300 million*, CNBC (Aug. 16, 2017), https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html.

[4] Kim S. Nash, Sara Castellanos & Adam Janofsky, *One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs*, WALL ST. J. (June 27, 2018), https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.

[5] Ellen Nakashima, *Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes*, WASH. POST (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[6] Alan Blinder & Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder*, N.Y. TIMES (March 27, 2018), https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

Atlanta's systems. The attack prevented 8,000 city employees from using their computers for five days.[7] Travelers in the Atlanta airport (the world's busiest airport) could not use the airport Wi-Fi even a week later.

Regulatory Approaches to Ransomware Preparedness. The Department of Health and Human Services (HHS) has released guidance on how to best prepare for and respond to ransomware attacks. HHS expects HIPAA-regulated entities not only to protect themselves against ransomware attacks, but also report such attacks when they occur.[8]

Additionally, the Department of Justice (DOJ) and Department of Homeland Security (DHS) have issued best-practice guidance for the private sector including ways to defend against ransomware, what to do once a computer/device has been attacked, and who to contact for help.[9] This guidance is targeted to organizations of all sizes. The DOJ/DHS guidance emphasizes protecting one's networks by educating personnel and taking preventive measures. Some preventive measures include implementing awareness and training programs, enabling strong spam filters, scanning all incoming and outgoing emails to detect threats, setting anti-virus and anti-malware programs to conduct regular scans automatically, and configuring firewalls to block access to known malicious IP addresses. The guidance also emphasizes the importance of backing

---

7 *Id.*

8 U.S. Dep't of Health & Human Servs., *Ransomware Guidance*, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html.

9 U.S. Dep't of Justice, *Ransomware Prevention and Response*, https://www.justice.gov/criminal-ccips/file/872771/.

up data regularly, securing the backups, and conducting an annual penetration test and vulnerability assessment. If a system is infected with ransomware, the guidance suggests removing the infected computer from the network immediately, powering-off devices that have not been completely corrupted, contacting law enforcement (the Federal Bureau of Investigation or U.S. Secret Service), and changing account passwords and network passwords after removing the system from the network.

* * *

As ransomware attacks become more prevalent and impactful in scale, it is no surprise that regulators and government agencies are beginning to act. This has become big business for hackers, and is apparently not beyond use by nation states. Companies and financial institutions must plan for these destructive threats just as they plan for breaches involving loss of personal data, and further should follow closely the changes to ransomware guidance and assessment tools regulatory bodies release. Companies should continually evaluate and update their strategies towards protecting themselves against ransomware attacks by preparing a business continuity plan that lays out in detail what the company would do in the event of a loss of access to email and/or other computer systems and how the company would respond to a ransomware attack. Developing and testing that plan is an important first step in minimizing the damage that a ransomware attack could cause.

Petya Ransomware Attacks

On June 27, 2017, a new wave of ransomware attacks quickly spread across the globe. The "Petya" malware encrypts and holds for ransom the entirety of an infected computer. Initial reports suggested that the malware targeted Ukrainian public infrastructure. Public and private entities in Russia, the EU, and the U.S. now reportedly have been affected. Like the recent WannaCry attacks, Petya is a reminder of the advisability of addressing ransomware as part of a broader cybersecurity program.

WHAT HAPPENED?

The initial intrusion appears to come through a malicious email attachment. The malware then exploits the same vulnerability targeted by WannaCry. Any computers that were unpatched following the WannaCry attacks thus remain vulnerable to Petya. Petya also attempts to harvest administrative credentials and spread horizontally through a compromised network.

Petya reboots the victim's computer and encrypts the master file table, rendering the entire system inoperable. This differs from previously observed malware that targeted individual files.

WHAT TO DO?

Our suggestions for action in the wake of Petya track our recent recommendations regarding WannaCry. Briefly: Above all, patch your systems directly at Microsoft's website. Go there directly. Ignore any unsolicited email you may have received that claims to offer a patch. Also, remember that even if you are able to unlock your files, the underlying malware will remain on the machine. Steps should be taken to eradicate it.

Consider also regularly backing up your data—and, just as important, testing your ability to actually operate from the backups. Remind employees to take special care not to click on unknown email attachments. Assess whether your technical defenses include current tools. Examples include: updated antivirus at system endpoints; firewalls to filter malicious traffic; network segmentation to stop or slow the spread of infection; and intrusion detection software to provide timely alerts of unusual traffic in your network. It is also prudent to line up outside help before any incident. This includes picking vendors (yes, including a law firm), and building law enforcement relationships.

We increasingly see specific ransomware preparations included in our clients' "tabletop" cyber response drills. Written incident response plans also increasingly address ransomware. Check your cyber coverage to see how a ransomware incident might or might not be covered. Collect and share threat intelligence through an Information Sharing and Analysis Center or similar cross-industry or multi-sector organization.

If you do get hit with a ransomware attack, legal as well as technical responses may be called for. The disruption that an attack can cause may trigger contractual or regulatory notifications. Consult counsel regarding the potential legal and practical ramifications of the decision whether to pay the ransom.

WHAT NEXT?

Petya's quick global spread suggests that post-WannaCry patching is, for many, still a work in progress. Regulators consider effective patch management a critical part of a risk-based information security program. Internal counsel can mitigate cybersecurity and regulatory risks by refreshing discussions surrounding ransomware

and patch management with their information security counterparts. This can also calm executive concerns.

This client update was originally issued on June 28, 2017.

Global Ransomware Attack: Essential Steps to Manage the Risks

As has been widely reported, a wave of ransomware attacks struck organizations around the world late last week, locking users out of their computer files unless and until they pay the hackers a ransom in Bitcoin. The attacks were alarming both because many hospital systems were heavily impacted, particularly in the U.K., and because of how rapidly they spread around the globe. The attacks are a reminder that organizations can and should take specific steps to address ransomware as part of their broader cybersecurity programs. Taking such steps is both good common sense and, increasingly, a legal mandate.

WHAT HAPPENED?

The attacks reportedly exploited a recently announced Windows vulnerability that a hacking group known as Shadow Brokers claimed to have stolen from the U.S. National Security Agency. Microsoft had released a patch for newer versions of its operating systems in April, but no patch was available for older operating systems on which many hospitals and others were running, such as Windows XP, until after the attacks commenced. Those who had failed to patch their systems, or who were running old operating systems, were vulnerable. The hackers behind this sadistically named their exploit the "WannaCry" or "WannaCrypt" ransomware.

As of today, public reports indicate over 200,000 victims of WannaCry ransomware in 150 countries. Russia, Ukraine, and Taiwan are the most heavily targeted countries to date, but the victims also include major institutions elsewhere, such as the National Health Service in the U.K. and Telefónica, the Spanish telecommunications company.

HOW BEST TO PREPARE AND RESPOND

Preparation for these incidents requires a combination of technical, legal and practical steps. As lawyers, we are not purporting to advise you on specific technical measures. We do encourage internal counsel who "own" cybersecurity issues to promptly incorporate, or refresh, the discussion of ransomware as part of their ongoing dialogue with information security colleagues.

- **Patch your systems**: The immediate priority should be to patch your systems. You can do so directly at Microsoft's website. Make sure you perform any downloads from the actual Microsoft site by going there directly, and not in response to any unsolicited email you may have received containing a link to install a patch.
- **Back up your data**: It is vital that your systems are backed up frequently and in a careful manner to prevent the ransomware from encrypting your backups as well. Attackers know that you will look to your backup systems to try to recover your files, and therefore commonly also try to lock you out of the backups to keep you on the hook to pay the ransom. Keep in mind that files saved only locally on infected systems are likely to be lost.
- **Immediately alert your employees**: "Phishing" emails, which attempt to trick the recipient into clicking on a malicious link or opening an attachment laced with malicious software or "malware," are a major attack vector for the spread of ransomware. Some early reports say that WannaCry has spread in part through phishing emails containing encrypted attachments. You should immediately remind your employees—as well as contractors who have access to your network—to be on high alert for emails, particularly with links or attachments, from unknown sources or that appear to be from known sources but include unusual requests. Although technical experts believe that

WannaCry spreads in an automated fashion once inside a victim's network, the initial compromise of the network likely comes from a phishing email.

- **Assess your defenses**: Evaluate your technical defenses with advice from both technical and legal experts. This includes, among other things, deploying updated antivirus at system endpoints, installing firewalls to filter malicious traffic, using network segmentation to stop or slow the spread of any infection, and using intrusion detection software to provide timely alerts of unusual traffic within your network.
- **Train for the worst**: Practice working through a ransomware scenario and how you would respond, including what legal, technical and broader business choices you would make. Drills should include a simulated re-start of your network using your existing backup systems, to help you assess how fresh and reliable those backups are as well as how quickly you can work around a ransomware attack by operating from the backups. This also provides an opportunity to consider whether certain key parts of your network or backups should be technically separated so that ransomware cannot spread to them.

  We often include ransomware scenarios in response drills, a/k/a tabletop exercises, to help our clients become efficient at responding to and managing these and other incidents. If your organization does not have a written cyber incident response plan ("IRP") that it tests regularly, now is a good time to begin adopting one. Given that speed of response is essential, the IRP, combined with testing, is a vital tool in avoiding any wasted time in escalating a potentially serious incident to the right personnel.
- **Line up outside help**: Arrange in advance the outside technical incident response vendor(s) you would use, and consider putting

their retainer in place through outside counsel to have the best chance of establishing privilege over investigation of and response to the incident. Many of our clients have these arrangements in place in advance so they do not waste precious time looking for, evaluating and engaging outside help during the storm of an incident.

- **Know your investigator**: To be ahead of the curve, you should know the face and cell phone number of the FBI, Secret Service, National Crime Agency or other law enforcement officials you would call with an urgent cybersecurity matter. Before you call, however, you should discuss with experienced in-house or outside counsel the pros and cons of engaging law enforcement and how to handle the interaction effectively. We often use our extensive law enforcement experience and relationships to help broker these discussions on behalf of our clients.
- **Assess insurance**: Assess your cyber insurance policy and refresh your understanding of the scope of coverage and the notification requirements it contains.
- **Stay current**: Stay on top of the latest cyber threats by participating in an industry platform such as an Information Sharing and Analysis Center ("ISAC") with members from your industry sector or an Information Sharing and Analysis Organization ("ISAO") that has members across sectors. The Financial Services ISAC or "FS-ISAC" is one example. More information is available through the National Council of ISACs.
- **Consider potentially required disclosures**: Although ransomware does not typically steal personal consumer data, the disruption it can cause to system operations may trigger contractual or regulatory notifications, depending on the nature of the business and its regulatory environment.

- **Pause before you pay**: In the event that your organization suffers a ransomware attack and you are faced with the choice of whether to pay a ransom, consult counsel regarding the potential legal and practical ramifications of the decision. Many organizations do choose to pay because the files the attacker has "padlocked" are business-critical and because the ransom amounts often are set at nuisance levels. But this choice is not without risks that you should consider in advance. For example, if backups are insufficient to avoid a need to pay, there may be other technical alternatives available to obtain the password or "key" to unlock your files.

WHY IS RANSOMWARE A LEGAL ISSUE?

Preparing for ransomware is increasingly seen not just as good technical practice, but as a matter of legal obligation. As we have previously reported, all entities covered by the U.S. Health Insurance Portability and Accountability Act ("HIPAA") have specific duties to prepare for and respond to ransomware attacks under guidance from the U.S. Department of Health and Human Services ("HHS"). HIPAA-covered entities, for example, must treat certain ransomware attacks as triggering disclosure obligations to affected individuals and to government agencies.

HHS also has joined the Department of Justice and the Department of Homeland Security to issue best-practices guidance for the private sector generally. A number of recent post-breach court cases have cited the victim entity's failure to follow best practices as potential support for a negligence claim or other cause of action against it.

This client update was originally issued on May 14, 2017.

New Federal Ransomware Guidance

Given that ransomware attacks are spiking sharply across corporate America, the U.S. Department of Health and Human Services has issued guidance on ransomware, which is instructive not just for healthcare entities but for enterprises in all sectors. The authors of this article discuss the guidance and what companies should do when faced with a ransomware attack.

The U.S. Department of Health and Human Services ("HHS") has just issued significant new guidance on ransomware. The guidance makes clear that entities subject to the data security provisions of federal healthcare law now have specific responsibilities both to guard against ransomware attacks and—in a departure from existing breach notification requirements—to report such attacks when they happen. Given that ransomware attacks are spiking sharply across corporate America, the HHS guidance is instructive not just for healthcare entities but for enterprises in all sectors.

RANSOMWARE FAQ

What is ransomware? Ransomware is a form of attack where the hacker does not steal your files, but encrypts them so you cannot access them. Then the hacker offers to sell you the encryption key, typically payable in the online currency Bitcoin. The usual demand comes with a deadline—after which time, the hacker threatens, the key will be discarded and your files will remain forever inaccessible.

If a low-tech metaphor helps: Think of the ransomware attacker as a sort of reverse "burglar," who doesn't break in to your house, but locks you out of it and demands payment to let you back in.

Why is the government taking action? Ransomware attacks are way, way up. There have been an estimated 4,000 attacks a day in 2016 to date, representing a 300 percent increase over 2015. Historically, ransomware attacks tended to be petty crimes directed at individuals and mom-and-pop organizations. But these attacks are now being directed more often, and with more success, at larger enterprises.

How do ransomware attacks happen? Ransomware gets onto an enterprise's system like any other kind of malware. "Phishing" attacks, where users unwittingly click on a malware-laden link or attachment in a seemingly innocent email, are a common vector. Hackers also may steal system credentials or exploit software vulnerabilities to install ransomware. Hackers who successfully launch their ransomware then typically post threatening messages on the screens of users at the victim entity. In one example cited by the Department of Justice, the hacker asserted that the users themselves had engaged in illegal activity and must pay a "fine." In another, the hacker stated that a ransom must be paid within a certain time period or "all your files will be permanently encrypted and nobody will be able to recover them."

Do victims pay the ransom? Often, yes. No comprehensive metrics are publicly available, but at least one study reports a 40 percent pay-up rate. It is a matter of public record that, earlier this year, Hollywood Presbyterian Hospital in Los Angeles paid its hacker 40 Bitcoin, or about $17,000. Even law enforcement is not immune; a Massachusetts police department has admitted that it paid a ransom to retrieve its work files.

Why pay? In that memorable line from the movie "Argo," payment of the ransom may be the victim's "best bad option." Enterprises face a tough choice when the encryption is not defeatable and the

padlocked files are business-critical. (How long can a modern hospital, for example, be offline before devastating consequences occur?) Compounding these difficulties, law enforcement agencies generally cannot find the cybercriminal fast enough to satisfy business demands, if they can find the criminal at all. (He or she may be overseas.) Moreover, the hackers frequently set the ransom at or about nuisance-value levels. And at least until now, there has been no disclosure requirement.

Add it all up, and payment of the ransom—however frustrating—can seem to be a reasonable cost-benefit calculation. As one Federal Bureau of Investigation ("FBI") official has said, "To be honest, we often advise people just to pay the ransom." (To be clear, the FBI's official policy is that victims should contact law enforcement. The new HHS guidance calls for reporting of ransomware attacks to the local FBI or Secret Service field office.)

Do hackers who are paid actually supply the encryption key? Often, yes. Again, metrics are hard to come by—but an FBI source has said that typically, "You do get your access back." Some ransomware attackers even ask you to rate them, like an Uber driver, so they can advertise to future victims that they have a track record of supplying the encryption key once paid.

There is not always honor among thieves. Published reports indicate that just this spring, a hospital in Wichita paid a ransom—but in return got only partial access to its files, together with a demand for an additional payment.

Isn't ransomware a crime? You bet. At a minimum, ransomware schemes run afoul of the federal computer crime statute, 18 U.S.C.

§ 1030, and particularly subsection (a)(7), which forbids hacking intended to extort something of value from the victim.

Up to now, what have been the legal obligations of ransomware victims? Few, if any:

- Most states have laws requiring disclosure of data breaches, but these laws ordinarily kick in only when data containing personal information is exposed or stolen—not when the data is simply made inaccessible.
- In specific situations, companies may be contractually required to give notice to their counterparties of certain cybersecurity events, including ransomware attacks.
- The U.S. Federal Trade Commission ("FTC") generally takes the position that maintaining poor cybersecurity can be an unfair business practice under Section 5 of the FTC Act. But the FTC has not yet applied this theory to try and hold a ransomware victim culpable. Informally, the FTC has indicated that it is focused on hacking cases that cause large-scale consumer impact—a description that does not fit the classic historical ransomware case, but might fit the emerging breed of enterprise-level ransomware attack.

THE NEW HHS GUIDANCE

The federal Health Insurance Portability and Accountability Act ("HIPAA"), has long imposed cybersecurity standards on covered entities and their business associates via the HIPAA Security Rule. The new July 11 guidance makes clear that HIPAA's cybersecurity standards will now be construed to apply to ransomware.

First, the guidance makes clear that those subject to HIPAA must "implement policies and procedures that can assist an entity in responding to and recovering from a ransomware attack."

These policies and procedures should include "maintaining frequent backups" and conducting periodic "test restorations," *i.e.*, measuring the enterprise's ability to actually function from backups if a ransomware attack were to limit access to regular systems. HHS also counsels organizations to "consider maintaining backups offline and unavailable from their networks." This is because of the propensity of ransomware attackers to target the backup files themselves—in effect, padlocking the garage door as well as the front door.

The HHS guidance specifies that all this is part of the larger obligation, under the Security Rule, to maintain a "data backup plan" that includes provisions for disaster recovery planning, emergency operations, analyzing the criticality of applications and data, and periodically testing contingency plans.

The long-standing HIPAA mandate to maintain "security incident procedures" will now be construed to require processes that will allow an organization to detect, analyze, contain, eradicate and recover from a ransomware attack. Ransomware attacks are now explicitly defined as "security incidents" triggering the obligation to deploy these procedures. Likewise, the long-standing requirement that a covered organization's workforce must receive appropriate security training now includes a requirement that the workforce be trained in how to detect and report malware so as to help ward off ransomware attacks.

Second, breach notification obligations may well now kick in under HIPAA even if other notification triggers, such as the states'

notification statutes, are not implicated. The guidance is quite clear that "the presence of ransomware ... is a security incident" for purposes of the Security Rule, and qualifies as a breach because unwanted encryption of personal health information ("PHI") by the ransomware attacker amounts to "acquisition" of that data by the attacker within the meaning of the Rule. Until now, ransomware and the payment of a ransom typically did not trigger breach disclosure obligations, and the guidance marks a significant departure from prior practice which may be a harbinger of change in other sectors.

Whether HIPAA disclosure procedures must be followed will be a case specific determination. But the general rule is that disclosure must occur unless the enterprise can show a "low probability" that PHI has been compromised. Traditional factors in this analysis include the nature and extent of PHI involved, whether the PHI was actually acquired or viewed, and the extent of risk mitigation. Under the new guidance, a "high risk of unavailability of the data, or high risk to the integrity of the data" is to be considered an indicator of compromise.

If the data encrypted by the ransomware attacker was previously encrypted by the data holder, that may cut against disclosure being required. Even then, though, the determination is case-specific—for example, a ransomware attack on an encrypted laptop could still result in a breach, for purposes of the Security Rule, if "the file containing the PHI was decrypted and thus 'unsecured PHI' at the point in time that the ransomware accessed the file."

WHAT'S AN ENTERPRISE TO DO?

Organizations subject to HIPAA of course must sit up and take notice of the new HHS requirements, and review their training

programs, technical protections, backup systems, and incident response protocols for compliance with the new guidance.

Organizations in all sectors of the economy can learn from the HHS requirements, however, and by doing so can reduce both their business and legal risks associated with ransomware. For it seems safe to say that once a major agency like HHS defines an obligation to detect, prevent, combat, and report ransomware attacks, then other legal authorities may converge around similar views.

The Department of Justice, the Secret Service and other federal agencies have joined with HHS to issue best-practices guidance for all enterprises. The interagency guidance is not limited to healthcare entities, and it closely resembles the new HHS mandates for HIPAA-covered organizations.

Also part of the chorus is the federal Computer Emergency Response Team ("US-CERT"), a technical expert entity based at Carnegie-Mellon University that recently issued its own guide, Ransomware and Recent Variants. CERT's guidance on risk mitigation closely resembles the interagency recommendations and HHS mandates.

Ransomware thus joins the growing list of cybersecurity threats that, under the law, potential victims are well advised to take specific measures to prevent, detect, and mitigate.

This article originally appeared in Pratt's Privacy & Cybersecurity Law Report *in October 2016.*

SEC / Public Companies

"All I'm saying is now is the time to develop the technology to deflect an asteroid."

Over the past few years, we have seen the SEC make cybersecurity a priority as it regulates material disclosure requirements and insider trading. Having created a dedicated Cyber Team in 2017, and with the issuance of updated guidance this past February, the SEC is in a position to hold companies to increasingly high standards.

Companies must take their internal policies and controls seriously to ensure their adequacy and effectiveness to combat against rising numbers of cybersecurity incidents. Overall, we have seen a shift from a risk-based and flexible approach to cybersecurity to one where companies must meet a baseline level of policies and procedures, and then exceed it as risk-based adjustments require. The SEC has made clear that they are prepared to bring enforcement actions when they find a company's controls or handling of a cybersecurity incident to be inadequate.

The SEC considers cyber security incidents and risks to be potential material nonpublic information ("MNPI"). To manage cyber MNPI, companies should have policies and procedures in place to prevent, detect, and assess cyber incidents in order to satisfy disclosure obligations under multiple reporting requirements, including Regulation FD, and controls and procedures requirements to safeguard against insider trading. Without the procedures in place to properly assess a cyber-related event, the SEC has indicated companies cannot effectively determine whether the incident is a material event requiring accurate and timely disclosure. The SEC has made it a priority to combat harm to investors from a failure to adequately disclose a material cyber incident or inadequate controls against insider trading based on a cyber incident or vulnerability.

For several years, we have advised companies on how to handle the initial disclosure and subsequent updates of a cybersecurity event. We have noted the need to consider the materiality of the event along with risks associated with initial disclosure based on incomplete data and companies' selective disclosure issues under Regulation FD. We have also highlighted reporting trends, including the increase in companies specifically referencing cyber-related events in annual and quarterly reports, and the connection between

disclosure and ongoing financial obligations related to cybersecurity events or in the event of major business or financing transactions.

More recently, we explained some of the ways in which the revised 2018 SEC Guidance would affect companies, underscoring the need to develop comprehensive controls and procedures related to cybersecurity and disclosure, and the importance of safeguards against trading by insiders based on material non-public information about cyber incidents or risks. This includes the ability to make timely decisions regarding whether circumstances call for a trading freeze for those insiders aware of a cybersecurity matter that constitutes material non-public information.

The SEC is also focused on the adequacy of the company's investigation of a cybersecurity matter and the company's timely disclosure based on the results. Earlier this year, the SEC settled charges against the company that was formerly Yahoo! with a $35 million penalty. This was the SEC's first case against a company for failing to adequately disclose a cybersecurity incident. Steven Peikin, Co-Director of the SEC Enforcement Division, stated that the SEC does not "second-guess good faith exercises of judgment about cyber-incident disclosure," but noted that a company's response "could be so lacking" as to warrant an enforcement action. The SEC took issue with Yahoo!'s failure to disclose a massive 2014 data breach for two years, specifically noting Yahoo!'s lack of disclosure in annual and quarterly filings and its failure to adequately investigate the incident. The SEC, through guidance and the Yahoo! action, has made clear that companies must provide a more detailed risk factor update, at least where the event is clearly material.

The Yahoo! settlement reaffirms the SEC's position that an ongoing investigation into a cyber-incident, internal or external, is not a

reason to avoid disclosure. A prolonged failure to disclose could result in an SEC enforcement action. We expect to see the SEC's focus on cyber security policies and protocols continue to evolve in the direction of greater disclosure expectations, with the possibility of further enforcement actions where a company's policies or response are "so lacking" as to warrant it.

Adequate and effective cybersecurity governance means robust governance and consideration of cybersecurity policies in a number of reporting and disclosure contexts. The SEC's Office of Compliance Inspections and Examinations announced general examination observations last year, providing several points of guidance that are, by now, assumed to be minimum expectations during exams:

- Policies must be detailed. General, vague guidance is not adequate.
- Employees need to be trained on the policies and held accountable for a failure to adhere.
- Policies must reflect actual practices. Annual or continuous reviews of security procedures must actually be carried out. A mandatory employee training policy needs to be enforced.
- High-risk findings from cybersecurity assessments need to be remediated, and policies must be in place to ensure this.
- Senior management must be engaged, and should vet and approve policies and procedures.
- Companies should consider upgrading obsolete technology.

The SEC's February guidance further suggests that all public companies should consider the impact of cybersecurity risks and incidents in the following settings:

- Reporting risk factors and MD&A

- Description of the business and legal proceedings pursuant to Regulation S-K & on Form 20-F
- Financial statement disclosures
- Describing the board's role in risk oversight
- Establishing and enforcing effective insider trading safeguards
- Complying with material disclosure requirements of Regulation FD

In this section, you will find a detailed collection of our recent cybersecurity updates and recommended practices for public companies.

New SEC Cybersecurity Guidance: Focus on Governance

On February 21, 2018, the SEC issued new Guidance regarding cybersecurity disclosure and governance requirements applicable to SEC reporting companies. In our earlier Client Update on this topic, we discussed the disclosure considerations addressed in the Guidance. In this Client Update, we focus on the cyber-related governance issues addressed in the Guidance.

CYBERSECURITY AND RISK GOVERNANCE

The Guidance addresses three governance topics in the context of cybersecurity: (1) the adoption and regular assessment of cyber-related disclosure controls and procedures; (2) the establishment of policies and procedures to address the risk of insider trading based on material nonpublic cybersecurity risks or incidents; and (3) compliance with Regulation FD when disclosing cybersecurity risks and incidents.

The SEC's focus on developing comprehensive policies and procedures related to cybersecurity and the need to guard against insider trading and selective disclosure is notable as those topics were not covered in the October 2011 guidance on cybersecurity issued by the Division of Corporation Finance.

Controls and Procedures

Building on the Sarbanes-Oxley Act and related SEC rules, the Guidance makes clear that appropriate and effective disclosure controls and procedures that enable companies to make accurate and timely disclosures of material events include "those related to cybersecurity." The Guidance notes that appropriate disclosure controls and procedures are essential to determine the potential

materiality of cybersecurity risks and incidents to the company and its business, financial condition, and results of operations, and thus are crucial to a company's ability to make any required disclosure in the appropriate time frame. Specifically, companies should regularly assess whether their disclosure controls and procedures:

- ensure that relevant information about cybersecurity risks and incidents is timely processed and reported to the appropriate personnel (*i.e.*, that they provide for open communications between technical experts and disclosure advisors, as well as up-the-ladder reporting to key decision makers);
- ensure timely collection and evaluation of information that is potentially subject to required disclosure or is relevant to an assessment of the need to disclose relevant developments and risks; and
- will appropriately record, process, summarize, and report the information related to the cybersecurity risks and incidents that are required to be disclosed in filings.

These types of controls and procedures should be generally consistent with disclosure controls and procedures that a public company already has in place with regard to the evaluation and disclosure of other material risks. However, it is worth noting that the nature of cyber-related matters and the intimate link with the technical side of the house may present new challenges when it comes to designing and implementing effective controls and procedures.

Sarbanes-Oxley CEO/CFO certifications regarding disclosure controls and procedures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and

incidents and for assessing and analyzing their impact. Similarly, the SEC expects a company's internal controls around financial reporting to be reasonably designed to capture the range and magnitude of the financial impacts of cyber incidents and ensure that those impacts are incorporated in the company's financial statements. The Guidance does not, however, explain how companies should assess the impact of a cyber incident on the effectiveness of its internal control over financial reporting.

Insider Trading

The Guidance encourages companies to consider how their policies, procedures, and controls account for and prevent trading on the basis of nonpublic information related to cybersecurity risks and incidents. Specifically, companies should review their insider trading policies and codes of ethics (as well as any related training) to assess whether they adequately guard against officers, directors, and other corporate insiders trading on the basis of (or otherwise misusing) material nonpublic information regarding cybersecurity incidents and risks.

Regulation FD

Given that information relating to cybersecurity incidents and risks may constitute material nonpublic information, companies may have disclosure obligations under Regulation FD in connection with nonpublic disclosures of those matters. Companies should review their policies and procedures relating to the selective disclosure of information (with a particular focus on their Regulation FD policies and related training). This review should assess whether these policies and procedures are sufficient to prevent selective disclosures of material cybersecurity incidents and risks in violation of Regulation FD.

FINAL THOUGHTS

The Guidance does not introduce novel concepts and expectations. Instead, the Guidance emphasizes the need for companies to assess and, as appropriate, revise their policies, controls and procedures to ensure that they effectively address cyber-related matters.

This client update was originally issued on March 12, 2018.

SEC Issues New Guidance on Public Company Cybersecurity Disclosure and Governance

Yesterday, the SEC issued new Guidance regarding cybersecurity disclosure requirements under the federal securities laws applicable to SEC reporting companies. The Guidance reinforces and expands upon October 2011 guidance issued by the staff of the Division of Corporation Finance.

The Guidance addresses two topics not covered in the 2011 guidance: (1) the importance of developing comprehensive controls and procedures related to cybersecurity, including those intended to facilitate an assessment of the materiality of—and consequent disclosure obligations stemming from—cybersecurity risks and incidents; and (2) the need for policies and procedures to guard against trading by insiders based on material non-public information about cyber incidents or risks and to ensure the timely disclosure of related material information.

SEC reporting companies with calendar-year fiscal years that are currently preparing 10-K and proxy disclosure should, assuming time allows, review the Guidance before finalizing their filings.

CYBERSECURITY GUIDANCE

Building on the 2011 guidance, the Guidance underscores the importance of robust and timely disclosure of cybersecurity incidents and risks, emphasizing that boilerplate disclosures (*e.g.*, we "may" be the victim of a distributed denial of service ("DDoS") attack) are likely insufficient where the company has in fact experienced an incident (*e.g.*, it has been the victim of a DDoS attack). The Guidance recognizes that disclosures need not reveal sensitive information about the company's protective measures—

lest they provide a roadmap to attackers—and suggests that companies consider the following factors when assessing disclosure obligations:

- The nature, extent, and potential magnitude of the risks and incidents, particularly as they relate to any compromised information or the business and scope of company operations;
- The range of harm that cybersecurity incidents could cause, including harm to a company's reputation, financial performance, and customer and vendor relationships; and
- The possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

As to timing, the Guidance recognizes that a victim company's cooperation with law enforcement to investigate a cyberattack might impact the scope and timing of disclosures, but warns that "an ongoing internal or external investigation—which often can be lengthy—would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." Notably, the Guidance reminds companies of their duty to correct and duty to update prior disclosures or omissions in light of facts learned through an investigation of a cyberattack.

At a more granular level, the Guidance suggests that companies consider the impact of cybersecurity risks and incidents in reporting risk factors, MD&A, description of the business and legal proceedings pursuant to Regulation S-K and on Form 20-F, in financial statement disclosures, and when describing the board's role in risk oversight.

The second half of the Guidance addresses three additional topics: (1) adoption and regular assessment of disclosure controls and procedures; (2) ensuring that policies and procedures are in place to address the risk of insider trading based on material non-public cybersecurity risks or incidents; and (3) ensuring compliance with Regulation FD when disclosing cybersecurity risks and incidents. Debevoise will shortly publish an additional update with further thoughts on those portions of the Guidance.

This client update was originally issued on February 22, 2018.

OCIE 2018 Examination Priorities Focus on Retail, but Private Fund Sponsors Still in Crosshairs

The Office of Compliance Inspections and Examinations ("OCIE") of the U.S. Securities and Exchange Commission recently published its 2018 examination priorities.[1] Consistent with Chairman Jay Clayton's priorities, the 2018 priorities focus on (i) protecting retail investors, especially seniors and those saving for retirement, and (ii) continuing current initiatives to reduce market-wide risks and improve market-wide infrastructure. However, private fund sponsors will likely continue to receive OCIE's attention.

PRIORITIES OF INTEREST TO PRIVATE FUNDS

OCIE will continue to concentrate on disclosures to investors regarding fees and expenses. In particular, the 2018 priorities state that OCIE will "focus on firms that have practices or business models that may create increased risks that investors will pay inadequately disclosed fees, expenses, or other charges." This category of firms includes private fund advisers that manage funds with a high concentration of investors investing for the benefit of retail clients—which OCIE views as including clients historically considered institutional, such as non-profit organizations and pension plans.

As in the past, OCIE will continue its scrutiny of never-before-examined investment advisers with higher risk profiles. Additional specific target areas relevant to private fund sponsors include:

---

1 *Available at* http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf.

- *Cybersecurity*. OCIE will examine for "governance, risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response."
- *Anti-money laundering*. OCIE will evaluate whether firms are "taking reasonable steps to understand the nature and purpose of customer relationships." OCIE will also assess whether firms are evaluating the robustness of their programs and filing Suspicious Activity Reports when appropriate.
- *Cryptocurrency, Initial Coin Offerings, and Blockchain*. OCIE will review safeguards against theft and misappropriation, and will focus on risk disclosures, including those associated with risk of loss, liquidity, price volatility, and fraud.

SENIOR RETAIL INVESTORS AND THOSE SAVING FOR RETIREMENT

OCIE will examine firms providing products and services directly to senior retail investors and retail investors saving for retirement, with particular focus on firms advising non-profit organizations, pension plans, and state, local and non-profit employees. OCIE will assess (i) compliance with disclosures, investor agreements, and internal policies that describe costs of investing, fees, expenses, and valuation, (ii) internal procedures used to supervise investment representatives to ensure that firms can identify manipulation of senior investors, and (iii) products and technological changes that pose a higher risk or that influence how advice is delivered. Other areas of focus include:

- *Wrap Fee Programs*. OCIE will examine (i) whether recommendations to invest or stay in wrap fee programs are reasonable, (ii) whether conflicts of interest are being disclosed,

and (iii) whether investment advisers are seeking and disclosing best execution costs.

- *Electronic Investment Advice*. OCIE will assess compliance programs with a special focus on computer algorithms that generate "recommendations, marketing materials, investor data protection, and disclosure of conflicts of interest"—in other words, "robo-advisers" and other online advisers.
- *Fixed Income Order Execution*. OCIE will evaluate whether broker-dealers have implemented best execution policies and procedures for municipal bond and corporate bond transactions.

EVALUATING MARKET-WIDE RISKS AND INFRASTRUCTURE

With respect to structural risks, OCIE notes its continued emphasis on existing initiatives regarding (i) clearing agencies, (ii) national securities exchanges, (iii) transfer agents, (iv) SCI entities (*e.g.*, registered clearing agencies, alternative trading systems, plan processors and exempt clearing agencies), and (v) oversight of regulated entities by FINRA and the Municipal Securities Rulemaking Board ("MSRB"). Other target areas include:

- *Mutual Funds and Exchange Traded Funds*. OCIE will focus on mutual funds that (i) show poor performance or liquidity, (ii) are managed by advisers with limited experience, or (iii) hold securities that are difficult to mark to market (*e.g.*, collateralized securities). Similarly, OCIE will scrutinize ETFs that (i) show poor secondary trading volume, (ii) risk being delisted, and (iii) may have to liquidate assets. In reviewing disclosures, OCIE will review conflicts of interest between advisers and index providers in instances where mutual funds and ETFs track customized indices.

- *Municipal Advisors and Underwriters*. OCIE will assess compliance with (i) qualification and continuing education requirements, and (ii) standards of conduct and duties as enacted by the MSRB.

CONCLUSION

- Private fund sponsors should continue to (i) review disclosures concerning fees, expenses and valuation, (ii) assess cybersecurity and anti-money laundering programs, (iii) update internal controls, and (iv) consider risks associated with cryptocurrency and blockchain.
- In addition to assessing the adequacy of disclosures concerning fees, expenses and valuation, firms providing products and services to retail investors should review disclosures concerning conflicts of interest and the costs of investing, provide reasonable investment recommendations, and look out for the protection of retail investors.
- OCIE will continue to evaluate market-wide risks and infrastructure and will assess regulatory compliance and corrective actions taken with a specific focus on market participants showing higher risk profiles.

This client update was originally issued on February 13, 2018.

SEC Releases Observations from Cybersecurity Examinations

On August 7, 2017, the Office of Compliance Inspections and Examinations ("OCIE") of the Securities and Exchange Commission issued a Risk Alert announcing observations from its second round of cybersecurity examinations of registered broker-dealers, investment advisers, and investment companies.[1] The observations were based on OCIE's examinations of 75 firms since September 2015, pursuant to its "Cybersecurity 2 Initiative"[2] which focused on six areas: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

OCIE identified "Issues Observed" (likely providing insight into future enforcement priorities), "Robust Controls" (giving some indication of OCIE's view of best practices), and "Summary of Examination Observations" (lending insight into the current state of the industry). Each is summarized below.

ISSUES OBSERVED

OCIE's guidance called out several areas for attention:

---

1 The full text of the Risk Alert is available through the OCIE webpage, https://www.sec.gov/ocie, or in PDF format at https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

2 See OCIE *National Exam Program Risk Alert*, OCIE's 2015 Cybersecurity Examination Initiative (September 15, 2015), *available at* http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

- Policies were not "reasonably tailored" because they provided only "general guidance" to employees, were vague, or failed to articulate procedures to implement the policies;
- Policies failed to reflect actual practices by, for example, calling for annual or continuous reviews of security procedures when in fact those reviews were conducted less frequently;
- Policies that required all employees to complete cybersecurity training when, in fact, the business did not ensure that training took place and did not take action against employees who failed to attend trainings;
- Contradictory policies;
- Use of outdated technology that is no longer supported by the vendor; and
- Failures to remediate high-risk findings from cybersecurity assessments (*e.g.*, penetration tests or vulnerability scans).

These findings provide a window into likely enforcement priorities. Accordingly, firms should consider reviewing policies—including those regarding cybersecurity training and monitoring—to ensure that they match actual practices. It would also be a good time to take stock of technology that has become obsolete and to consider upgrades. Finally, firms should assess whether they have procedures in place to ensure remediation of vulnerabilities discovered during assessments.

ROBUST CONTROLS

OCIE identified certain practices as "robust," giving some sense of OCIE's view of best practices, including:

- Maintenance of an inventory of data, information, and vendors, including classifications of the risks of each service provider.

- Detailed cybersecurity-related instructions, including policies and procedures relating to penetration tests, security monitoring and system auditing, access rights, and reporting.
- Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities, such as vulnerability scans of core IT infrastructure and patch management policies.
- Established and enforced controls to access data and systems, such as detailed "acceptable use" policies for the firm's networks and equipment, restrictions and controls for mobile devices that connect to the firm's systems, logs of third-party vendors' activities on the firm's networks, and immediate termination of access for terminated employees.
- Mandatory employee training for all employees at on-boarding and periodically thereafter.
- Engaged senior management who vetted and approved the policies and procedures.

SUMMARY OF EXAMINATION OBSERVATIONS

The staff observed that most firms had implemented the following cybersecurity practices, giving some insight into the state of the industry:

- Written policies and procedures addressing cyber-related protection of customer/shareholder records and information.
- Periodic risk assessments of critical systems to identify threats and consequences of cyber incidents.
- Penetration tests and vulnerability scans on critical systems.
- Systems or tools to protect personally identifiable information.
- Regular system maintenance, including the installation of software patches to address security vulnerabilities (although a

few firms had not yet installed a significant number of system patches that included critical security updates).
- Policies and procedures addressing cyber-related business continuity planning and Regulation S-P requirements that firms adopt written programs for the protection of customer records and information.
- Policies and procedures addressing cybersecurity and Regulation S-ID requirements that firms adopt written programs to prevent identity theft in connection with certain consumer accounts.
- Response plans for addressing access incidents, denial of service incidents, and authorized intrusions. The staff noted that fewer than two-thirds of advisers and funds maintained such plans.
- Cybersecurity organizational charts and descriptions of cybersecurity roles and responsibilities for the firm's workforce.
- Authority from customers/shareholders to transfer funds to third-party accounts.
- Vendor risk assessments, typically required at the outset of a relationship and in many cases performed at least annually thereafter.

The Risk Alert underscores OCIE's prioritization of cybersecurity risk management and continues a trend of increasing regulatory scrutiny of the details of firms' cybersecurity programs. Leading regulators such as the SEC now expect a comprehensive cybersecurity program of policies, procedures, and technical controls, and they continue to transform best practices into regulatory requirements.

This client update was originally issued on August 14, 2017.

SEC Approves CAT Plan While Mitigating Data Security Concerns

On November 15, 2016, the Securities and Exchange Commission ("SEC") voted and approved the consolidated audit trail ("CAT Plan"), a comprehensive trade reporting system that will allow regulators to access all trade activity in U.S. equity and options markets.[1] The CAT Plan would build a central repository that receives, consolidates and retains the trade and order data reported, owned by a Delaware limited liability company (the "CAT NMS LLC"). We discussed the details of the proposed CAT Plan earlier this year when the rule was proposed.[2] This update highlights the SEC's approval of the CAT Plan with certain amendments stemming from industry feedback, along with a brief discussion of the inherent data security concerns.

WHAT CHANGED IN THE FINAL PLAN?

Compared to the May 2016 proposal, the SEC responded to industry feedback by amending the plan with the following changes:

- **Data Security**: The proposed CAT Plan gave the Plan Processor[3] the responsibility for security and confidentiality of all CAT Plan data received and reported to the central repository. In the

---

1 Press Release, SEC, SEC Approves Plan to Create Consolidated Audit Trail (Nov. 15, 2016). *See also* SEC Release No. 34-79237 (Nov. 15, 2016).

2 *The SEC Proposes the CAT Plan, but at What Cost?*, Debevoise & Plimpton LLP (May 17 2016).

3 Plan Processor means the Initial Plan Processor or any other Person selected by the Operating Committee pursuant to SEC Rule 613 and Sections 4.3(b)(i) and 6.1, and with regard to the Initial Plan Processor, the Selection Plan, to perform the CAT processing functions required by SEC Rule 613 and set forth in the CAT NMS Plan. SEC Release No. 34-77724 (Apr. 27, 2016).

approved CAT Plan, the SEC strengthened several data security requirements, including with respect to personally identifiable information("PII"). Data security has been a significant concern to the public and is discussed in greater detail below.

- **Clock Synchronization**: In the proposed plan, each participant and industry member is required to synchronize its business clocks to within 50 milliseconds of the time maintained by the National Institute of Standards and Technology ("NIST"), at a minimum and consistent with industry standards. The final CAT Plan tightened the clock synchronization standards for self-regulatory organizations ("SROs") to within 100 microseconds of the time maintained by the NIST. This would require SROs to assess industry standards for clock synchronization based on the type of market participant or system, rather than the industry as a whole, and reflect that refined assessment annually in a report submitted to the SEC. The change is intended to enable regulators to better sequence order events across multiple exchanges.
- **CAT Governance**: The proposed plan outlined the composition of the advisory committee to the CAT NMS LLC. As part of the approval, the SEC expanded the membership of the advisory committee to include an additional investor representative and a representative of a service bureau that provides CAT Plan reporting services.
- **Retirement of Existing Regulatory Reporting Systems**: The final CAT Plan accelerated the deadline for SROs to submit proposals to retire regulatory data reporting systems that will be rendered obsolete by the CAT Plan. The change is intended to reduce the burden on broker-dealers reporting duplicative trade data to multiple systems.

LOOKING FORWARD

Ongoing Concern: Data Security

Data Security has been a significant concern for the industry in designing the CAT Plan. More broadly, regulators have made cybersecurity a focus across the financial services industry. Several regulators have published proposed regulations and guidance on the topic.[4] In response to industry feedback, the SEC strengthened the data security requirements of the CAT Plan for the Plan Processor who is tasked with implementing the requirements.

The final CAT Plan establishes various data security requirements regarding connectivity, encryption, and access to PII. The Plan Processor is required to comply with the NIST Cybersecurity Framework and the SROs to maintain information security protocols. In addition, an annual evaluation of the information security program is required. The Plan Processor is required to evaluate the central repository's information security program at least annually. Further, the Plan Processor is responsible for developing access controls to the central repository, a comprehensive information security program and designating a Chief Information Security Officer, who would have various cybersecurity responsibilities. Comments made by industry groups note that the central repository of the CAT Plan may be a significant

[4] *See A Week of Hot News in Cybersecurity and Data Privacy*, Debevoise & Plimpton LLP (Mar. 8, 2016); *New York's Proposed Cyber Regulations: Implications and Challenges*, Debevoise & Plimpton LLP (Sept. 15, 2016); *SFC Cybersecurity Review of Internet/Mobile Trading Systems*, Debevoise & Plimpton LLP (Oct. 17, 2016); *Federal Financial Regulators to Propose Enhanced Cyber Risk Management Standards*, Debevoise & Plimpton LLP (Oct. 25, 2016); *UK Government Launches Five Year National Cyber Security Strategy*, Debevoise & Plimpton LLP (Nov. 2, 2016).

target for cyber criminals and hackers.[5] Specifically, SIFMA reiterates that it would be "essential that the CAT have robust protections for the massive volume of sensitive transaction data and [PII] it will track and store, which will include social security numbers for every person with a brokerage account."[6]

While the final CAT Plan contained additional data security requirements, financial institutions should continue to monitor this issue, especially once the Plan Processor is selected and begins to design the data security protocols.

Next Steps

Within the next two months the SROs must select a Plan Processor to implement the CAT Plan; including developing policies and building a central depository. SROs will be required to begin reporting to the central depository within one year, large broker-dealers will begin reporting the following year and small broker-dealers the year after. Industry members should start thinking about compliance and technology changes that will be requirement at each firm, and how this initiative may be integrated with other recent regulatory changes.[7]

This client update was originally issued on November 21, 2016.

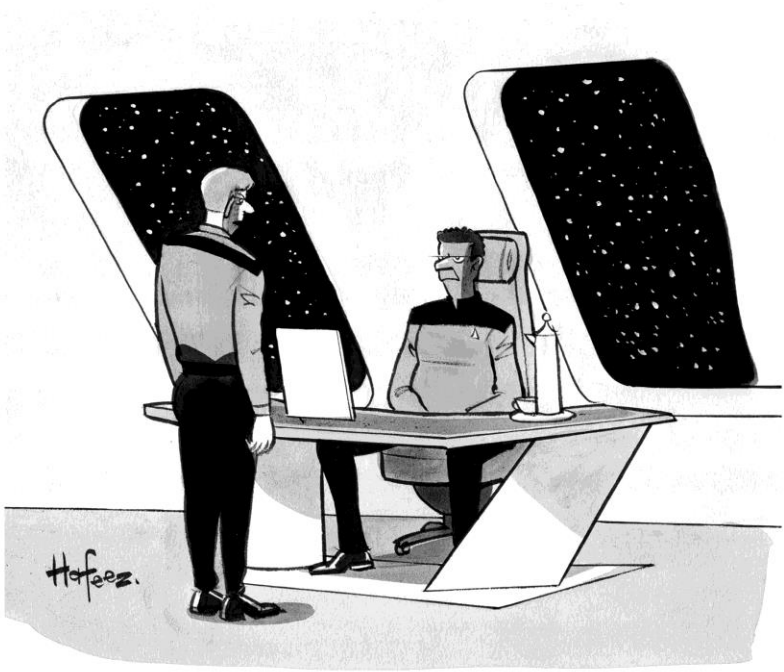
---

5 For comments made to the proposed CAT Plan see the SEC's website.

6 Press Release, SIFMA, *SIFMA Highlights Concerns with the Proposed Plan for Developing a CAT System*, (July 18, 2016).

7 *See Final DOL Fiduciary Rules Simplify Some Mechanics, but Retain Core Principles . . . and Flaws*, Debevoise & Plimpton LLP (Apr. 13, 2016).

GDPR and Cross-Border Data Privacy



"Bad news, captain. The ship's computer has been sharing all our personal data with the Romulans."

The EU's General Data Protection Regulation ("GDPR") has significantly altered many companies' obligations and responsibilities regarding the personal data they collect, store, and process. Businesses subject to GDPR have continuously been adjusting their practices in order to ensure compliance with the

comprehensive and expansive mandates set forth in the GDPR since it went into effect about a month ago, though it is clear from surveys that compliance is far from universal even after the GDPR took effect on May 25, 2018. The GDPR replaced the United Kingdom's 1984 Data Protection Act and the European Union's Data Protection Directive, and unified diverse data privacy laws in Europe under one governing piece of legislation. The GDPR's reach is broad: its guidelines essentially apply to every company that in the course of conducting business with EU-based data subjects, collects, stores, or processes their personal data. And in the context of data breaches, the GDPR's 72-hour reporting window is far shorter than what most businesses are used to. The GDPR represents a significant shift in the world of data collection and privacy, and businesses need to carefully understand the way they collect and handle data in order to comply with its requirements.

You don't have to do business in the EU or have employees in the EU to be potentially subject to the GDPR's requirements (though how an EU regulator would enforce the regulation against a company outside the EU remains an open question). By its terms, the GDPR applies to any company that obtains the personal data of an EU resident—whether directly, from its own customers or employees, or indirectly, by processing another company's data in the context of providing them services or monitoring them. How EU-based data protection authorities will interpret and enforce these extraterritorial provisions is still unclear. Even if the GDPR's provisions are interpreted narrowly, it could be onerous and risky to process data differently in different locations of a business. Whether businesses that operate both in Europe and elsewhere will choose to handle all of their data processing in accordance with the mandates of the GDPR or employ separate data processing schemes is also an evolving question.

The GDPR represents a fundamentally different way of thinking about personal data than U.S. companies are used to. In the U.S., personal data is generally viewed as belonging to the business that acquires it, which would for the most part be free to do with the data as it pleased. For businesses that fall under the GDPR, that is no longer the case. The GDPR gives substantial power to EU residents to govern what companies do with their personal information. When the original purpose for obtaining the data is fulfilled, the business no longer has an absolute right to retain it. The GDPR permits individuals to request that their data be moved to another institution, or deleted. Businesses are devoting significant resources to GDPR compliance.

The GDPR speaks in broad terms and there is no simple checklist that can be completed in order to ensure GDPR compliance. There won't be a point where a business will receive a certification indicating that its work is finished and it has reached "compliant status." Compliance is an ongoing process, and requires dynamic and adaptable policies to ensure success. Keeping the principle in mind that the individual retains autonomy over his or her information is helpful in implementing a sufficient set of best practices that minimizes risk and liability.

Consent and transparency are both incredibly important under the GDPR. The U.K.'s Information Commissioner's Office ("ICO") stresses, for example, that businesses should disclose to individuals the names of third parties that will process their data. In line with the theme of individual sovereignty over their data, this consent must be obtained with equality of bargaining power, and in the context of genuine choice and control over data. Consent must be rigorously documented and periodically evaluated. It is also helpful to remember that consent is not the only lawful basis for processing

an individual's data under the GDPR, and it may not be the most appropriate legal basis. Considering and pursuing a different legal basis not only provides an alternative to the difficult task of obtaining informed consent, but also ensures legal grounds for processing an individual's data remain even if they revoke their consent. Regardless, the GDPR places a significant emphasis on disclosure and transparency. Making a good faith effort to inform consumers of what data you are collecting and what you are doing with it is essential. This ensures their consent is actually informed. The ICO has issued a series of user-friendly, practical compliance guides to GDPR that businesses would do well to consult.

The high end of the penalty range provided for in the legislation—up to 4% of global annual turnover, in the event of particularly serious noncompliance—made big headlines leading up to its effective date. But since its enactment, there has been no indication that the GDPR penalties will be levied indiscriminately (much as maximum fines were not typically imposed under the EU's prior regime). The most important thing is to make a good faith effort to comply. Before the GDPR's effective date, the ICO stated that it is more interested in using the "carrot over the stick" method. While the GDPR provides for very harsh fines for violations, these serve as a ceiling, not a floor.

Despite the extensive requirements in the GDPR, they are very much achievable. This is true even for the 72 hour reporting requirement in the event of a data breach, to which much attention (and apprehension) has been devoted by affected businesses. A business assumes much less risk if it is at least working towards implementing programs to ensure compliance than it does by considering compliance a lost cause. As long as businesses use their best efforts to comply with GDPR guidelines, we do not expect to see penalties higher than under previous regimes.

While stringent, the GDPR requirements are manageable, and compliance is possible for firms of all sizes. The articles in this section provide our advice for smoothing the transition to GDPR compliance.

You Want *What*?: Responding to Individual Requests Under the GDPR

With the EU General Data Protection Regulation ("GDPR") in force for less than two months, many companies are already experiencing an increase in requests from individuals seeking to obtain a copy, or request correction or erasure, of their personal data under Articles 15 to 17 of the GDPR.

Do we have to respond? Yes. A response is required even if the response is that the company will not honour the request because a relevant exemption applies.

Can we ask for additional information? Yes. If you have any doubt that the requester is who he/she claims to be, ask for information necessary to ascertain the requester's identity or to confirm how the requester has interacted with your company in the past. Where appropriate, you can also ask the requester to limit the scope of the request or otherwise engage with him/her to understand the "root cause" of the request. Individual rights requests are rarely made in a vacuum and usually form part of a wider context—for example, a customer service complaint or an employment dispute. Understanding that context may help narrow the request or eliminate it altogether.

How quickly do we have to respond? The standard response period under the GDPR is one month from receipt. That can be extended by two months where necessary, taking into account the complexity and number of requests. Where possible, it is best to keep to the one-month response period. In our experience, extending the response time is likely to lead to an expectation on the requester's part that the request would be fully honoured and, where the request is for a

copy of personal data, an expectation that significant amounts of data would be produced.

Do we need a form, policy, or procedure for individual requests? GDPR does not require these, but it makes good sense to have them if you expect to receive numerous requests. An internal policy or checklist setting out the process can help ensure consistent, GDPR-compliant responses. Conversely, there is no requirement that the requester use a specific procedure or form to submit a request. Nor is there any obligation on you to have an online form available for that purpose. Deciding whether to publish such a form requires balancing cost and benefit. Responses submitted via a publicly available form may be clearer, but you may get more of them.

When can we refuse to comply with a request, in whole or in part? Unfortunately, this question does not lend itself to a short answer. The GDPR sets out a number of exceptions and limitations on individual rights requests, as does EU Member State domestic legislation (this being one of the few areas under GDPR where Member States have some discretion to set their own rules). These may include circumstances where personal information of other individuals would have to be disclosed, where the request is manifestly unfounded or excessive, or where compliance would compromise your compelling interests or public interest, among others. Careful consideration needs to be given to these factors to determine the best basis, if one exists, to object to a particular request.

This client update was originally issued on July 18, 2018.

Draft EU Guidelines on Cross-Border Data Transfer

Earlier this month, the Article 29 Data Protection Working Party (a coalition of European Union member states' data protection regulators) issued draft Guidelines on when EU personal data can be transferred to non-EU countries that, according to the EU authorities, do not adequately protect personal data. The Guidelines interpret Article 49 of the EU General Data Protection Regulation ("GDPR"), which deals with these types of transfers. Although not legally binding, the Guidelines suggest how EU data protection authorities will interpret Article 49. The comment period for the Guidelines is open until 26 March 2018, providing businesses and other stakeholders with an opportunity to influence the final version.

Under the GDPR, EU personal data can be transferred outside the EU only if the recipient country is certified by EU authorities as providing an adequate level of data protection, or if EU-approved safeguards for such protection, such as standard contractual clauses or binding corporate rules, have been implemented. Article 49 provides exemptions (or "derogations") in certain limited circumstances.

The Guidelines bring some good news to companies required to produce EU personal data to civil litigants or enforcement authorities outside the EU, and in the United States in particular. However, the Guidelines maintain the Working Party's restrictive interpretation of other derogations. That means that the GDPR, as currently interpreted, likely will restrict cross-border data sharing even in some cases when important interests like cybersecurity are at stake.

THE GOOD NEWS: "ESTABLISHMENT, EXERCISE OR DEFENCE OF LEGAL CLAIMS" DEROGATION MAY ALLOW FOR GREATER INFORMATION SHARING WITH U.S. AUTHORITIES AND CIVIL LITIGANTS[1]

Under Article 49(1)(e) of the GDPR, EU personal data can be transferred to the U.S. if it is necessary for the establishment, exercise, or defence of legal claims. The Working Party's interpretation of the analogous article in the Data Protection Directive (the GDPR's predecessor) offered only one example where this derogation "appears to" apply: an active U.S. litigation against a company by its employee that requires transfer of that employee's personal data from the EU. Any such transfer also had to comply with relevant international conventions, including the Hague Convention on Taking of Evidence. Unsurprisingly, many practitioners expressed doubt that this provision could be used as a basis for complying with pre-trial civil discovery requests or in non-adversarial dealings with U.S. authorities.

The new draft Guidelines take a more expansive view of this derogation. They state that a transfer of EU personal data to the U.S. could be made when it is necessary for a U.S. criminal or administrative investigation, for the purposes of defence or to obtain "a reduction or waiver of a fine legally foreseen," or for pre-trial discovery. The Guidelines interpret Article 49(1)(e) to require a "formal, legally defined process" in the U.S., but emphasise that this "covers a range of activities."

---

[1] The Guidelines and Article 49 of the GDPR apply to all transfers to countries that do not provide an adequate level of data protection. In practice, however, they tend to target transfers to the U.S., given the breadth of U.S. civil discovery and the extraterritorial reach of U.S. law. Accordingly, we refer to transfers to the U.S. throughout this update.

Assuming that the draft Guidelines do not materially change before they are formally adopted, Article 49(1)(e) could serve as a basis for producing information to the U.S. Department of Justice ("DOJ") or the U.S. Securities and Exchange Commission ("SEC") in connection with the Foreign Corrupt Practices Act or other white collar matters. In fact, the Working Party appears to have had just such matters in mind; the Guidelines specifically refer to antitrust, corruption, and insider trading investigations. That said, the requirement that "formal procedures" have been instituted (or at least be impending) suggests that voluntary self-disclosures to the DOJ or the SEC are unlikely to be covered.

To rely on Article 49(1)(e) to transfer EU personal data, companies must show that the transfer is necessary. The Guidelines state that U.S. authorities' "mere interest" in the data or "possible 'good will'" to be obtained from the production will not meet that standard. If a U.S. subpoena calls for the production of a specific EU individual's personal data—for example, if the individual is suspected of wire fraud or money laundering—transfer of that personal data presumably would qualify. On the other hand, producing personal data of other EU individuals who may have transacted with the alleged fraudster, but who are not themselves targets of the U.S. subpoena, might run afoul of the necessity requirement. Such data may need to be anonymised or pseudonymised before it is transferred. Where the EU personal data is not explicitly requested by the U.S. legal process but is likely of interest to the requesting party, companies may consider engaging with the U.S. authorities or civil litigants to modify the relevant requests to meet the requesters' goals while satisfying the GDPR.

By making room for these considerations, the draft Guidelines provide a path for multinational companies to navigate between U.S. information requests and the GDPR, a path that previously was difficult to discern.

THE BAD NEWS: PUBLIC INTEREST, VITAL INTERESTS, AND COMPELLING LEGITIMATE INTERESTS BASES FOR DATA TRANSFERS REMAIN HIGHLY RESTRICTIVE

The Guidelines fail to offer a broader interpretation of other bases for EU personal data transfer to the U.S. As before, the Guidelines limit the "public interest" derogation to instances when the transfer itself is in the public interest of the EU, for example, because of an agreement between the EU and the U.S. to share particular types of information. A general shared interest (for example, that both the EU and the U.S. seek to combat terrorism or money laundering) is insufficient.

Likewise, the "vital interests of the data subject or others" basis for data transfers continues to be limited to medical emergencies and other life-and-death situations when the relevant individual is incapable of giving consent. The Guidelines do not consider other serious risks to individuals that may be prevented or ameliorated through cross-border data sharing. Cyberattacks are a prime example. As financial institutions and other businesses fighting against cyber-threats can attest, a timely and free exchange of attack-related data, which may include personal data of suspected perpetrators or their victims, is crucial to preventing or stopping the attack.

The Guidelines appear to consider cyber-related data transfers under Article 49's "last resort" derogation—that for "compelling legitimate

interests" of the data transferor. They state that a business may be "compelled to transfer the personal data in order to protect its organisation or systems from serious immediate harm." The Guidelines emphasise, however, that the "compelling legitimate interests" must be those of the data transferor, not of the data importer or any other third party. This would prevent an EU financial institution hit by a cyberattack from transferring relevant EU personal data to a U.S. financial institution to prevent the attack from spreading to the latter. That transfer would be in the interest of the data importer, not the data transferor. While one can hope that this is not the type of a situation where the EU data protection authorities would take action against the data transferor, the fact remains that Article 49 provides little cover for such transfers.[2]

It is possible that the Working Party will reconsider its interpretation of Article 49, either during the comment period or subsequently. In an unusual move, the Working Party explicitly stated that it would review and update the Guidelines, if needed, based on practical experience of their application. In the meantime, companies would be well advised to consider other bases for cross-border information sharing, such as by executing standard contractual clauses among relevant industry participants.

Debevoise advises businesses, both in and outside of the EU, on all aspects of GDPR preparedness.

This client update was originally issued on February 21, 2018.

---

[2] Article 49 places additional restrictions on the "compelling legitimate interests" derogation, including that any such interests must be weighed against the rights of the affected individuals and that any transfers under this derogation must be notified to the relevant data protection authority and affected data subjects.

Draft GDPR Transparency Guidelines Issued: What Does Your Privacy Policy Need to Contain?

Late last year, the Article 29 Working Party (the "Working Party") issued detailed draft guidance (the "Guidelines") on transparency under the EU General Data Protection Regulation (the "GDPR"), which comes into force in May 2018. These Guidelines, which will be finalized following a consultation process, contain the Working Party's interpretation of the mandatory transparency information that must be provided to a data subject by way of privacy policy or other disclosures.

One of the express requirements of the GDPR relates to how businesses communicate their use of a data subject's personal information to that data subject at the point of data collection or consent, typically via a privacy policy or notice. Getting this right is crucial. Businesses will need to examine their current privacy policies and other disclosures closely, and consider whether these need revising not just in the light of the GDPR, but also to factor in the requirements listed in the Guidelines, which elaborate on existing GDPR provisions. While the Guidelines will not be binding, data protection authorities may take a dim view of businesses which fail to comply with the Guidelines without good reason, given that representatives from all of the EU data protection authorities are part of the Working Party. Businesses that fail to comply with the information duties under the GDPR will face fines of up to the higher of 4% of annual worldwide turnover or EUR 20 million.

THE WORKING PARTY GUIDELINES

First, what information must businesses include in their privacy polices?

- *Identity and contact information for the controller/data protection officer* (where applicable[1]): this allows the data subject to easily identify who the controller is and should, where possible and practicable, include several methods by which the controller can be contacted (*e.g.* phone number, email address, postal address).
- *Purposes and legal basis for processing*: companies should include the legal basis relied upon for processing alongside the purposes for which the data is processed. The Guidelines do not specify whether the privacy policy must list the legal basis for each category of data processed (*e.g.*, names, telephone numbers, e-mail addresses).
- *Legitimate interests*: where legitimate interests are relied on by the controller or third party as the legal basis for processing, the specific legitimate interests need to be expressly stated in a way the data subject can understand. Businesses should also consider, as best practice, providing the data subject with information on how the data controller balances its own interests against those of the data subject. Businesses should carefully consider how to execute this in practice; succinctly summarising the "balancing test" while also ensuring it is easily understandable might seem challenging, but is worthwhile where practicable in order to demonstrate compliance with, for example, the GDPR's accountability principle.
- *Recipients or categories of recipients of personal data, including third parties, joint controllers and processors that receive data*: the default position is that information must be provided on any named recipients. In many cases, for example where the controller engages various data processors, the identity of which may

[1] The Working Party has prepared specific guidance on Data Protection Officers (WP 243, last revised and adopted on 5 April 2017).

change from the time to time, this task may be onerous and not always practicable. If the controller elects to provide categories of recipients instead of individual names, the controller must be able to show why it did so and provide as much information as possible in the privacy policy, such as information about the type of recipient (by reference to the activities it carries out) and the industry, sector and sub-sector, as well as where the recipients are located.

- *Transfers of data to third countries, along with the safeguards in place and where copies of such safeguards can be found* (*e.g.* via a link): the privacy policy should specify the basis for any data transfer outside the European Economic Area (*i.e.* binding corporate rules, adequacy decision, standard contractual clauses and derogations), along with a list of third countries to which data will be transferred. The Guidelines state that the list must be exhaustive.
- *The retention period*: the Guidelines state that it is insufficient to state, in general terms, that personal data will be held for as long as is necessary for the purposes for which it was processed. Businesses can use statutory requirements or industry guidelines as a means of assessing how long personal data should be kept, but the overarching purpose is to allow a data subject to assess the relevant storage periods, depending on the categories of data provided. Where the data is being held due to an ongoing commercial, business or employment relationship, it may not be possible for the controller to specify an exact retention period, but the data subject should have sufficient information to be able to determine the period.
- *Data subjects' rights*: a privacy policy should include information on how a data subject can access, rectify, erase, restrict processing of, object to the processing of and port their data. These rights

must be explicitly brought to the data subject's attention. While stated in the Guidelines, although not expressly required by the GDPR, this information may need to be accompanied by explanations on what the right involves and how it can be exercised.

- *How a data subject can withdraw consent*: not only does this need to be contained within the information provided to data subjects, but businesses need to ensure that their systems and processes can actually affect the withdrawal of consent as easily as it was given.
- *The right to complain*: data subjects need to be made aware of their right to complain to the relevant supervisory authority in the event of an infringement (actual or alleged) of the GDPR.
- *Use of mandatory fields*: online forms need to indicate clearly which fields are mandatory and which are optional, as well as the consequences of not completing the mandatory fields. For example, in an employment context there may be a contractual requirement to provide certain information to an employer.

Second, the GDPR requires businesses to provide information to data subjects in a way that is "concise, transparent, intelligible and easily accessible." What does this mean for privacy policies in practice?

- Information on the processing of a data subject's personal data must be presented in an efficient and succinct manner, in order to avoid "information fatigue." Using layered privacy statements is a good way of ensuring a privacy policy is easily navigable and user-friendly. Alternative means available to online businesses include "just-in-time" contextual pop-up notices, 3D touch or hover-over notices and privacy dashboards.

- Businesses can make their privacy policies easily and readily accessible by making the information available on the same page on which personal data is collected and by clearly signposting it. The Guidelines consider that combining a privacy policy with other terms and conditions or only providing a link to the privacy policy on the first page of the website will be insufficient.
- The privacy policy must be easy to understand. Businesses should establish who their intended audience(s) are and what the average member's level of understanding may be, taking particular care where their goods/services target children or vulnerable members of society. User panels can be used to test whether an intended audience understands the privacy policy relevant to the processing of their personal information.

Third, businesses will need to monitor their compliance with the transparency requirement regularly throughout the life cycle of processing (for example when data breaches occur) and not only at the point when data is collected from the data subject or otherwise obtained.

Fourth, complying with the current draft Guidelines does not necessarily ensure future compliance. The Working Party will publish updated Guidelines along with a *FAQ* section once it has analysed the responses to its transparency consultation, and the UK Information Commissioner's Office will continue to revisit its approach as future EU guidelines and best practices develop post-May 2018. Businesses should do the same to ensure they meet the regulators' evolving expectations as the GDPR comes into force and is enforced.

Draft GDPR Transparency Guidelines Issued:
What Does Your Privacy Policy Need to Contain?

Debevoise advises businesses, both in and outside of the European Union, on all aspects of GDPR preparedness.

This client update was originally issued on 16 January 2018.

GDPR – 12 Months to Go – 10 Steps You Should Consider Now

INTRODUCTION

There is just one year to go until the General Data Protection Regulation (the "GDPR") comes into full force on 25 May 2018, replacing the existing EU Data Protection Directive (the "Directive"). Data privacy and cybersecurity have been increasingly in the news and on regulators' agendas, and there is no reason to believe this trend will diminish. In this client update, we set out ten key issues businesses should consider now to prepare for the changes the GDPR will bring.

1. Determine if your company is subject to the GDPR

Like the Directive, the GDPR will apply to all companies that have a presence in the European Union, but it also significantly expands the territorial scope of the EU data protection regime. Specifically, even companies with no EU presence will have to comply with the GDPR if they process personal data of "data subjects" who are in the EU in connection with (1) "offering of goods or services" to data subjects (no payment required); or (2) "monitoring" of the data subjects' behaviour online, for example, for the purposes of subsequent profiling. The "offering of goods or services" prong of the GDPR's territorial scope is very fact-specific and requires careful consideration of a non-EU company's business model vis-à-vis customers located in the EU, including whether that company's online presence is likely to be perceived as envisaging serving individuals located in the EU.

2. Consider hiring a Data Protection Officer

The GDPR will require companies whose core activities require large-scale "regular and systematic monitoring" of data subjects or

large-scale processing of their sensitive data to appoint data protection officers ("DPOs"). Some EU data protection authorities, such as the CNIL in France, have gone even further and strongly recommend that all companies that process EU personal data appoint DPOs to ensure GDPR compliance. Identifying a qualified person to serve as a DPO may be a challenging task, given the extensive expertise and capabilities expected of this role. A 2016 study estimated that the GDPR would create 28,000 vacant DPO positions, and companies that must (or want to) appoint a DPO should begin the recruitment process without delay. Companies that are not obliged to appoint a DPO, but wish to appoint a person responsible for data protection compliance, should consider creating a position with a title other than a "DPO" to avoid unnecessarily imposing mandatory obligations of the DPO on that individual.

3. Update fair processing and privacy notices

The GDPR aims to increase transparency about how personal data is handled, expanding the types of information that organisations have to provide to individuals to ensure fair and transparent processing of their data. Privacy notices or policies published on websites and elsewhere may need to be updated to include information about, among other things: (1) data retention periods; (2) safeguards relating to data transfers outside the EU; (3) contractual or statutory consequences of refusal to provide personal data; and (4) contact information of the company's DPO, where applicable. That information must be provided in "concise … and easily accessible form, using clear and plain language"; data protection jargon and overly technical language should be avoided. Although providing additional information may not be overly onerous in and of itself, identifying existing deficient notices that require updating may be a significant task for some businesses.

4. Assess consent

Consent is one of the bases for legitimately processing personal data under the Directive and will remain one under the GDPR. The GDPR, in contrast to some Member States' existing regulations, toughens the definition of a valid consent and casts doubt on whether much of pre-GDPR consent-based personal data processing will remain valid.[1] If your company relies on data subjects' consent for processing their data, make sure that those consents remain valid post-GDPR, including that they are (1) specific to the particular processing activity; (2) voluntary; and (3) active (requiring a positive step rather than inaction on the data subjects' part).

5. Consider conducting a data protection impact assessment

Data protection impact assessments will become mandatory under the GDPR where large-scale processing of sensitive personal data or data subjects' profiling are involved. These are, in essence, data privacy risk assessments, aimed to determine whether a company is adequately addressing its data protection risks and to remediate as warranted. As with the appointment of DPOs, organisations should consider whether conducting an impact assessment is advisable as a tool for ensuring GDPR compliance even if it is not strictly required under the GDPR.

6. Implement an incident response plan

The GDPR introduces, for the first time, a pan-EU data breach notification obligation, requiring companies that suffer qualifying

---

1 *See, e.g.*, D&P Client Update, *UK Information Commissioner's Office Issues GDPR Consent Guidance: What Business Should Know and Do*, 7 March 2017; *available at* http://www.debevoise.com/insights/publications/2017/03/uk-information-commissioners-office-issues?wb48617274=4A20E446.

personal data breaches to notify relevant EU supervisory authorities and, in some cases, affected individuals. Notifications must be made without undue delay and in any event within 72 hours, a time frame that, practically speaking, means that companies subject to the GDPR need to have a cyber incident response plan ("IRP") in place before a breach occurs. Organisations subject to the GDPR should also set out in their IRPs the process for determining whether a breach has to be notified and, if so, the procedure for making the notifications.

7. Review and update data processing agreements

Companies should review existing contracts with third parties that process personal data on their behalf to ensure that they are valid post-GDPR. Such contracts should include a range of requirements on data processors, including assistance with and reporting of data breaches, technical and organizational measures the data processor must undertake to safeguard the data, and audit rights.

8. Be prepared to comply with new and enhanced individual rights

The GDPR enshrines a host of new individual rights—including the rights to data erasure ("right to be forgotten") and data portability and the right not to be subject to automated decision-making (for example, profiling)—and expands existing rights, for example the right to receive, on request, information about the processing of an individual's personal data. Many of the new and expanded individual rights aim to increase individuals' ability to control the way in which their personal data is handled. As such, companies should be prepared for the possibility that they would be receiving a significantly higher number of requests and complaints from data subjects. It is most prudent to prepare for that ahead of time by

setting out policies and procedures for responding to such requests and complaints (or reviewing policies and procedures already in place).

9. Identify your lead supervisory authority

Under the GDPR, one data protection supervisory authority will take the lead on investigating data protection issues that implicate several EU Member States for companies established in the EU. Although more guidance on this subject is anticipated, it is likely that, for companies operating in more than one EU Member State, the lead supervisory authority would be the one covering the jurisdiction of the company's headquarters and/or the centre of the corporate decision-making. EU data protection authorities have explicitly discouraged "forum-shopping" for lead supervisory authorities, but it remains worthwhile for companies to consider who its lead supervisory authority would be and whether more than one supervisory authority could credibly claim that title. For companies that are at higher risk of scrutiny (*e.g.*, those that process large quantities of personal data), it is then prudent to establish good working relationships with the lead supervisory authorities and ensure that they keep up to date with those authorities' guidance and expectations.

10. Train staff

With all the new provisions that GDPR introduces, it is essential to ensure that company staff—and in particular the employees dealing with individuals' personal data—are appropriately trained. In most cases, that training must extend not just to the DPO or the employees specifically tasked with data protection compliance functions, but also IT, Legal, Human Resources, Marketing, and

other functions whose activities inadvertently can put companies at risk of violating the GDPR.

CONCLUSION

While the GDPR is still 12 months away from coming into force, organisations that are or may be subject to its jurisdictions should spend that time to prepare, including by implementing the steps outlined above. We expect regulators to be unsympathetic to those who are not compliant by 25 May 2018, given that the final text of the GDPR has been available since 2016 and has been widely discussed and analysed since then. The time to consider GDPR's impact on your business, and take the appropriate steps, is now.

This client update was originally issued on May 23, 2017.

UK Information Commissioner's Office Issues GDPR Consent Guidance: What Business Should Know and Do

The UK Information Commissioner's Office ("ICO") has issued detailed draft guidance on consent as a basis for dealing with personal data under the EU General Data Protection Regulation ("GDPR"), which enters into force on 25 May 2018. The ICO has also launched a consultation on the guidance open until 31 March 2017.

Businesses that will be subject to the GDPR come May 2018 should: (i) ensure their GDPR preparations reflect the ICO's guidance; and (ii) consider using the consultation to shape the ICO's interpretation of the GDPR and ensure it protects individuals' rights without placing undue burdens on business, within the GDPR's constraints.

THE GDPR & CONSENT

The GDPR overhauls data protection across the EU and beyond (where non-EU businesses offer goods or services to, or monitor activities of, EU-based individuals). Both businesses in the EU and those that target the EU should ensure they are ready to meet the GDPR's enhanced data protection requirements. Further, it appears likely that the UK government will pass legislation mirroring, or very similar to, the GDPR, which will apply after "Brexit." GDPR compliance is, therefore, likely to be relevant even for businesses operating only within the UK.

Becoming GDPR compliant will not, for most businesses, involve reinventing the wheel. The GDPR builds upon many existing legal rules and best practices. Nevertheless, failing to devote sufficient resources to GDPR-readiness could cost organisations dearly.

Companies that breach the new rules will face fines of up to the higher of 4% of annual worldwide turnover or €20 million.

While individuals' consent remains a legal basis for processing personal data, the GDPR ratchets up what is required to obtain valid consent; it must be "freely given, specific, informed and unambiguous" in the form of "a statement" or "clear affirmative action."

Pre-ticked opt-in boxes, never a favourite of EU regulators, plainly will become a thing of the past. What else will change?

THE ICO GUIDANCE

First, businesses should examine the sufficiency of existing consents. Consents obtained under the current data protection regime will remain valid, provided they meet the new GDPR requirements. If they do not, businesses should obtain fresh consents or put in place alternate bases for processing of that data (and communicate that basis to the relevant individuals).

Businesses should take note that consent from a counterparty to a contract must be obtained separately from other contractual terms and conditions and should not generally be a precondition to signing up to a service. This means, for example, that in an online transaction, the consent to future marketing contacts generally should be obtained through an affirmative tick in a box separate from the consent box for the transaction itself.

However, for many business purposes, such as handling customer data to provide goods or services or employee data to manage employment relationships, consent is not required because other

provisions of the GDPR can (and should) be relied upon—notably, necessity for the performance of a contract or employer's legitimate interests.

Second, consent requests must be carefully drafted and tailored to their specific context. Organisations should proactively direct individuals' attention to consent requests, and keep them separate from general terms and conditions. At a minimum, a request should identify the data controller's name, reasons for the data collection, how the data will be used, and who will use it. Consent requests also must explain that the individuals can withdraw their consents at any time and how they can do it.

Such transparency is paramount. The ICO stresses, for instance, that businesses should disclose to individuals the names of the third parties that will process their data. In the ICO's view, a reference to a generic class of organisations is inadequate because it does not give individuals sufficient oversight and control over their data.

Third, organisations should ensure that their consent procedures give individuals genuine choice and control over how their data is handled. The ICO suggests that consent would be difficult, although not impossible, to obtain in the employment context, given the disparity in bargaining power between the employer and the employee. This will make it difficult to obtain valid consent in employment contracts. Instead, employers may need to rely on other bases for processing their employees' data, such as necessity for the performance of the employment contract or the employer's legitimate interests. If they do not, they may face a challenge in showing that consent was "freely given."

Similarly, organisations may find it difficult to rely on consent as a basis for processing where, if the consent is not given, they will nevertheless process the data on other grounds. Relying on "fall-back" provisions where the validity of consent is questionable could breach the GDPR's requirements of fairness and transparency.

Therefore, organisations should determine whether consent is the most appropriate and efficient basis for processing each particular category of personal data they control. Where businesses rely on non-consent grounds for processing, they should document and communicate those grounds in accordance with the GDPR's requirements, such as via privacy notices.

Fourth, organisations will have to periodically review whether existing consents remain valid. As noted above, the GDPR gives individuals the right to withdraw their consents at any time, and data processing based on a consent that has been withdrawn must cease (though pre-withdrawal data processing is unaffected).

The ICO also advocates proactive consent management by data controllers. For example, it recommends that organisations refresh consents every two years in most cases. As such, businesses should consider having systems in place to alert them when new consents might be required.

Fifth, businesses must fully document consents to create an audit trail. Under the GDPR, organisations relying on consent to process data must be able to demonstrate that the individual actually consented. Business records should indicate which individuals gave their consents, what information they were provided, when and how they consented, and whether they withdrew their consents. For

example, such records could include a time-stamped capture of the individual's consent form and a copy of the privacy policy or notification in place on that date.

Sixth, complying with the current guidance does not necessarily ensure compliance in the future. The ICO acknowledges that it will continue to revisit its approach as future EU guidelines and best practices develop post-May 2018. Businesses should do the same to ensure they meet the regulators' evolving expectations as the GDPR comes into force and is enforced.

Debevoise is available to assist organisations wishing to contribute to the ICO's consultation and advises businesses, both in and outside of the EU, on all aspects of GDPR preparedness.

This client update was originally issued on March 7, 2017.

Privacy Shield *Not* Trumped

President Trump's January 25 Executive Order on immigration is attracting a great deal of attention, to say the least. While the order is plainly focused on the Middle East, some commentators have suggested that the order has made collateral damage of Privacy Shield—the protocol for transfers of personal data from the European Union to the United States that came online in August 2016. We respectfully submit that such commentary is off point. Privacy Shield faces challenges but is alive and well.

WHAT IS PRIVACY SHIELD?

Privacy Shield is the mechanism negotiated by US and EU authorities to allow companies to bring personal data of EU origin west across the Atlantic for storage and processing in the US. It aims to solve a basic problem: the EU generally recognizes stronger personal rights to data privacy than the US. Accordingly, the EU generally does not allow transfers of personal data to less protective jurisdictions unless the transfer occurs pursuant to an approved exception or mechanism.

Under Privacy Shield, companies certify that they will follow certain standards for the protection of EU citizens' personal data and will submit to enforcement in both the US and the EU. In exchange, companies are free to move personal data from the EU to the US—a key protection for companies doing business on a global basis. Over 1500 companies have self-certified thus far.

Privacy Shield replaced the now-defunct Safe Harbor, a predecessor data transfer system that was invalidated by the European Court of Justice in 2015 due to concerns about the level of privacy protection in the US. The ECJ stated that US government authorities had

"access on a generalized basis" to personal data in the hands of private companies. EU approval of Privacy Shield was based in part on certain commitments by the US government. For example, the Federal Trade Commission promised to pay particular attention to Privacy Shield enforcement. Congress also passed, and President Obama signed, the Judicial Redress Act of 2015. That statute allowed the US Attorney General to extend the protections of the Privacy Act of 1974 to citizens of certain other countries. Outgoing Attorney General Loretta Lynch, as one of her last acts in office, extended those protections to citizens of EU member countries, effective February 1, 2017.

The Privacy Act creates no broad right to privacy in the US. Rather, as noted in the Justice Department's helpful overview, the Privacy Act merely establishes certain information handling practices for US federal agencies. These include that agencies can only disclose citizens' personal information for certain purposes or with the individual's consent.

DOES THE NEW EXECUTIVE ORDER AFFECT PRIVACY SHIELD?

Commentators concerned about the impact of President Trump's January 25 Executive Order on Privacy Shield have pointed to Section 14 of the Order:

> Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.

On this basis, European privacy advocates—such as Jan Philipp Albrecht, a member of the European Parliament—have claimed that the EU must immediately suspend Privacy Shield and issue sanctions against the US. The US tech and business press have echoed the concerns: "Trump order strips privacy rights from non-U.S. citizens, could nix EU-US data flows," reads a typical headline.

Such commentary notwithstanding, the text of Section 14 actually has no direct effect on the Privacy Shield framework. It should first be noted that the ultimate fate of Privacy Shield strictly speaking rests not with any unilateral action of the White House, but with EU authorities—particularly the ECJ, which will hear a pending legal challenge to Privacy Shield's validity. Moreover, Section 14 does not change US companies' ability to meet their obligations under Privacy Shield, because Section 14's instructions do not apply to these companies. The text of Section 14, and the text of the Privacy Act, is directed to "agencies"—that is, US government entities—and not US companies. Nor does the Executive Order undo Attorney General Lynch's designation of the EU and its member states as covered under the Judicial Redress Act.

In short, the Privacy Shield remains intact. US companies are still free to self-certify under Privacy Shield, and meet the resulting obligations, without worry that this might run afoul of Section 14 of the Executive Order.

Concerns remain. As noted, privacy advocates in the EU have already begun to mount legal challenges to Privacy Shield in the courts there. We have conferred with our friend and former colleague Professor Joel Reidenberg, a leading global privacy scholar and director of the Center for Law and Information Policy at Fordham Law School. Professor Reidenberg says: "Both sides of the Atlantic

are heavily invested in the Privacy Shield and the other legal mechanisms to bridge the differences in transborder privacy protections. While this Executive Order does not revoke the Privacy Shield, it does create uncertainty over the new administration's commitment to Privacy Shield. At the same time, the Executive Order is likely to be a factor against the future validity of the Privacy Shield in the upcoming EU court decisions and is likely to push greater scrutiny by EU data protection authorities of data transfers to the United States."

WHAT MIGHT US COMPANIES DO NEXT?

Privacy Shield remains effective. Companies that qualify for it may still wish to consider whether to self-certify. Companies may also wish to consider a belt and suspenders approach—*i.e.*, self-certifying under Privacy Shield, while also adopting one or both of the alternative mechanisms for EU-to-US data transfers. The alternatives are the Binding Corporate Rules and Standard Contractual Clauses; these, like Privacy Shield, formally obligate US-based data recipients to provide EU-style protection for EU personal data. Standard Contractual Clauses, like Privacy Shield, are currently subject to legal challenge in the EU. The benefit of the belt and suspenders approach is that if any one of these mechanisms is ultimately invalidated by the EU courts, a company that has adopted multiple mechanisms could still rely on any that survive these legal challenges.

This client update was originally issued on February 1, 2017.

Private Litigation

"Madame Zelinski can provide an even more accurate reading with your date of birth and social security number."

It has become commonplace and is now generally expected that a flurry of litigation will follow the announcement of most significant data breaches. These lawsuits generally fit into three categories: (1) class actions filed on behalf of individuals whose data allegedly was compromised; (2) claims by financial institutions that claim they suffered a loss; and (3) derivative suits filed by shareholders. In this section, we focus primarily on the first category—the evolving landscape for companies defending against customer class actions.

These claims are not a new phenomenon, but the outcomes for certain plaintiffs have grown somewhat more favorable in recent years. Historically, these cases were often dismissed in the very early stages of litigation, on motions to dismiss, frequently because plaintiffs could not plead any harm, and therefore they had no standing to sue. To have standing, a plaintiff must have suffered harm resulting from the defendant's conduct. In data breach cases, this is challenging in both regards: first, many customers cannot even prove fraud or identity theft after a data breach; second, even those who do suffer fraud cannot necessarily trace the cause of the fraud to any data breach in particular. These twin challenges have meant that breached companies frequently could get rid of class action suits on motions to dismiss.

The Supreme Court passed up the opportunity to provide real clarity on the issue of standing in the data breach context in its decision in *Spokeo v. Robins*. Presented with the chance to crisply declare a clear requirement to plead real world harm or face dismissal, the Court instead held in vaguer terms that a plaintiff must plead an injury in fact that is both concrete and particularized. Though it held that a mere procedural violation is insufficient, the Court did not elaborate on what is necessary to meet the standard. As discussed further in this section, the lower courts have split on the question of what constitutes standing, specifically, whether increased risk of future identity theft can be sufficient. Despite the split, plaintiffs are now much more successful in defeating motions to dismiss than they had been in the past.

The practical result of this is that companies, faced with the risk and expense of discovery and protracted litigation, settle the class actions. For example, Anthem reached a $115 million settlement with consumers after over two years of litigation and a failed motion

to dismiss. After Anthem announced a data breach involving the personal information of approximately 80 million people, over one hundred class action suits were filed and consolidated. Anthem moved to dismiss based in part on plaintiffs' lack of standing. The court denied the motion, rejecting the standing argument and finding, among other things, that plaintiffs sufficiently pled injury by alleging that they suffered a "loss of the benefit of the bargain"—essentially that they got less than they paid for because Anthem did not implement the security measures the parties contracted for. On the issue of causation, the court found the causal connection was plausibly established by alleging that (1) the plaintiffs were enrolled in a particular Anthem health plan, (2) they provided their PII to Anthem, (3) their PII was compromised as a result of the breach, and (4) their PII was used for illicit financial gains. The judge rejected the notion that companies can avoid responsibility for data breaches by relying on the multitude of other data breaches that could also put people at risk.

The settlement agreement between Anthem and the class action plaintiffs included monetary and business commitments from Anthem. In addition to establishing a $115 million settlement fund, to provide plaintiffs with two years of free credit monitoring and reimburse any out-of-pocket costs resulting from the breach, Anthem committed to adopting additional information security safeguards and providing plaintiffs with a copy of independent assessments of those safeguards.

Other recent class action settlements include:

- Kimpton Hotel & Restaurant Group LLC reached a proposed settlement with the class impacted by the breach of a server that processed payment cards used by approximately 150,000 Kimpton

guests. If the settlement is approved, Kimpton will reimburse consumers for out-of-pocket expenses up to $600,000, implement certain data security measures, and pay attorneys' fees.

- The parent company of AshleyMadison.com, an infidelity website for married people, agreed to pay $11.2 million to settle a class action resulting from a breach affecting approximately 37 million users.

Several forces may be at work in the trend of increasing plaintiff success. First, plaintiffs may simply be getting better at articulating the injury suffered, and thus have been able to persuade certain courts that the serious risk of identity theft and fraud following a breach and the costs associated with mitigating this harm—such as credit monitoring, credit freezes, and cancelling credit cards—is actual harm. Additionally, as the steady stream of data breaches continues, some courts seem to be growing impatient with corporations and increasingly sympathetic to plaintiffs.

Whatever the reasons, the trend in the last few years is clear: the financial risk to companies that suffer data breaches is only increasing. In addition to evaluating and strengthening information security to prevent breaches, companies should prepare for how best to respond to an eventual breach to minimize legal exposure. Among other things, involving counsel from the early stages of incident response and taking measures to protect the privilege of the investigation and response can minimize risk if the company finds itself at the discovery phase of litigation.

Privacy Law Summary

Data breach law continues to evolve rapidly, with courts and regulators across the United States demanding increasingly high standards of protection for many kinds of data. Regulators have continued to bring enforcement actions in a broad variety of circumstances, and courts are continuing to lower the bar for plaintiffs to state claims.

All 50 states have now enacted their own data breach notification statues and many states continue to expand, revise, and update their own definitions of personally identifiable information and procedures for handling data breaches. In this shifting legal and regulatory landscape, any entity that stores or maintains customers' or employees' personal information—which is to say, virtually every company—would do well to closely monitor developments in federal and state privacy law to ensure their own data systems and practices are adapting to the new environment. This article provides a summary of some recent developments in federal and state cases across the country.

One significant trend we're monitoring is the shift to a more permissive approach towards standing, allowing more plaintiffs to survive a motion to dismiss. In the past, violations of procedural rights were generally held insufficient for plaintiffs to establish Article III standing, and courts were inclined to read statutes conveying substantive privacy rights narrowly.

Courts used to be skeptical of many kinds of alleged harm or risks of harm following a data breach, dismissing suits where the risk or injury was too hypothetical or removed. Following the Supreme Court's decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016),

however, and as the news fills up with more and more stories of data breaches and their consequences, courts appear to be increasingly willing to read statutory privacy protections as protecting substantive rights. Further, courts seem to be giving greater weight to plaintiffs' claims of increased risks of harm resulting from a breach, expanding the set of circumstances in which plaintiffs can survive a motion to dismiss.

Two recent cases highlight the impact of these trends:

- In *Dieffenbach v. Barnes & Noble*, 887 F.3d 826 (7th Cir. 2018), the Seventh Circuit took Spokeo's standing approach and applied it to the damages context. The Seventh Circuit held that injuries that established standing—like money spent on credit-monitoring services and time spent resolving related issues—were sufficient to justify money damages, removing a hurdle for plaintiffs in maintaining suits with little direct economic harm.
- Following *Commonwealth of Massachusetts v. Equifax Inc*., 2018 WL 3013918 (Supr. Ct. Suffolk Apr. 2, 2018), entities that own, license or store data in Massachusetts are facing increased obligations to rapidly detect and address flaws in their software in order to protect data against a broadening range of reasonably foreseeable information security risks. In *Equifax*, the Suffolk County Superior Court held that while the data breach itself did not violate Massachusetts law, the Attorney General had adequately pleaded that the failure to safeguard consumer data could violate the law. Under Massachusetts' Standards for the Protection of Personal Information, a company has a duty to address reasonably foreseeable information security risks and to maintain reasonably up-to-date versions of its software. In particular, the court pointed to a factual allegation concerning whether Equifax failed to patch a security vulnerability in its

database software in a reasonable time after it became aware—or should have become aware—of the vulnerability.

In addition, courts across the United States continue to increase the pressure on entities that own, store, or license data in a variety of contexts:

- Standing:
  - *In re Zappos.com Customer Data Security Breach Litigation*, 888 F.3d 1020 (9th Cir. 2018). Reversing the lower court, the Ninth Circuit held that plaintiffs sufficiently alleged an injury in fact under *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), based on a substantial risk that the Zappos hackers would commit identity fraud or identity theft. In doing so, the court affirmed that *Krottner* is still good law after *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). In *Krottner*, the Ninth Circuit held that the increased risk of identity theft associated with a data breach was a credible threat of real and immediate harm that satisfied Article III standing. The *Zappos* court found that *Krottner* was not irreconcilable with *Clapper* since the "especially rigorous" standing analysis in *Clapper* arose in a national security context, and the claimed injury there was dependent on a "speculative multi-link[ed]" chain of inferences. Here, there were no national security implications and the sensitivity of the personal information, combined with its theft, was enough to conclude that plaintiffs adequately alleged an injury in fact.
  - There is a growing circuit split on the question of whether increased risk of identity theft alone suffices to establish an injury in fact sufficient for standing purposes. The Sixth, Seventh, Ninth, and D.C. Circuits have found standing based on increased risk of identity theft, while the Fourth and

Eighth Circuits have found such injury too speculative.[1] The Second Circuit had yet to address this issue directly, but in *Whalen v. Michael Stores Inc.*, 689 F. App'x 89 (2nd Cir. 2017), the court held that a plaintiff who failed to allege that sensitive personal information like a Social Security Number was stolen, and whose credit card was cancelled shortly after the data breach, could not plausibly plead an increased risk of future fraud. Although *Whalen* cited to a Sixth Circuit case in holding the plaintiff's allegations insufficient to support standing, the *Whalen* decision does not necessarily mean that the Second Circuit will find an increased risk of identity theft sufficient to confer standing.

- *Bassett v. ABM Parking Services*, 883 F.3d 76 (9th Cir. 2018). The Ninth Circuit held that a parking garage customer claiming that the garage ran afoul of the Fair Credit Reporting Act by printing credit card expiration dates on receipts failed to allege a concrete injury in fact under the standard set in *Spokeo*. The court held that because only one copy of the receipt existed which was only ever in Bassett's possession, and Bassett never was the victim of identity theft, there was no injury. The panel held that because Bassett's private information was not disclosed to anyone but himself, no substantive right was invaded. Additionally, he did not sufficiently allege any risk of harm as he could shred the offending receipt along with any remaining risk of disclosure.

---

[1] Compare *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018); *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016); with *In re SuperValu, Inc.*, 870 F.3d 763, 769–71 (8th Cir. 2017); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017). In a pre-*Spokeo* decision, the First Circuit held that exposure of PII alone would not suffice to establish standing. *Katz v. Pershing, LLC*, 672 F.3d 64, 79–80 (1st Cir. 2012).

- *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735 (W.D.N.Y. 2018). The court held that customers who claimed their data had been exposed—but not misused—as a result of a 2015 data breach at Excellus BlueCross BlueShield had alleged an injury sufficient to establish Article III standing, reversing the courts' earlier decision on the same issue.
- *In re Facebook Biometric Information Privacy Litigation*, 2018 WL 2197546 (N.D. Cal., 2018). The court denied Facebook's motion to dismiss Plaintiffs' claims, in which Facebook had argued Plaintiffs lacked Article III standing because they failed to allege a concrete injury in fact. In rejecting Facebook's arguments, the court found that the Biometric Information Privacy Act (BIPA) vested Illinois residents with the right to control their biometric data by, requiring notice before collection and a right to withhold consent. Because the Illinois legislature created BIPA's notice and consent procedures to protect residents' privacy rights, the court concluded that Facebook's violation of the procedural rights resulted in the "quintessential[] . . . intangible harm that constitutes concrete injury in fact."

- What information constitutes PII:
  - *Eichenberger v. ESPN, Inc.*, 876 F.3d 979 (9th Cir. 2017), furthers a circuit split over which test to use to determine what constitutes personally identifiable information. Although the case specifically arises under the Video Privacy Protection Act (VPPA), the basic concept—what information "identifies a person"—is implicated in a wide variety of contexts. The Third and Ninth Circuits have adopted the "ordinary person" test, which examines whether the information disclosed readily permits an ordinary person to identify a particular individual as having watched a video. By comparison, the First Circuit uses a "reasonable and

foreseeable" test, asking whether the information is reasonably and foreseeably likely to reveal which videos a person viewed.

- Privacy in the medical context:
  - *Hancock v. County of Rensselaer*, 882 F.3d 58 (2nd Cir. 2018). In this case brought by employees of a county jail whose medical records were made available to other employees, the Second Circuit held that the Fourteenth Amendment's due process clause protects individuals from arbitrary intrusions into their medical records by government actors. Because that protection must be balanced against the government's interests in each particular case, the Second Circuit remanded the case for further fact development, directing the district court to evaluate plaintiffs' privacy claims in light of the fact that the defendants offered no reason for the breach and to consider whether the defendants acted with malicious intent.

Information Security Programs Play a Central Role in Target Data Breach Settlement

On May 23, 2017, Target Corporation ("Target") reached an $18.5 million settlement with the Attorneys General ("AGs") of 47 states and the District of Columbia. The agreement resolves the states' investigation into Target's 2013 data breach and is the largest ever multistate data breach settlement with regulators.

THE BREACH

In 2013, cyber criminals obtained network credentials from one of Target's third-party vendors and used the credentials to exploit weaknesses in Target's point-of-sale systems. The breach affected more than 41 million customer payment cards and exposed the contact information of over 60 million customers.

Prior to this settlement, Target had settled with a class of banks for more than $59 million in a final and approved settlement. Target had also reached a $10 million settlement with a consumer class impacted by the breach, but the 8th Circuit reversed the settlement, remanding to the District Court for consideration of class certification issues.

THE SETTLEMENT TERMS

Besides requiring Target to pay $18.5 million to the states, the settlement agreement requires Target to implement technical, administrative, and physical safeguards commensurate with the size of Target's technical infrastructure, types of personal information maintained, and nature of its business. Key provisions require that Target:

- encrypt cardholder and personal information;

- segment payment card data information from the rest of the computer network;
- implement greater controls over who can access its network, including requiring two-factor authentication for some accounts and mandating password rotation;
- develop a risk-based penetration testing program;
- employ a Chief Information Security Officer (CISO), who is responsible for reporting to and advising the corporation's CEO and Board of Directors on the corporation's security risks; and
- obtain an independent, third-party assessment of Target's information security program within one year of the settlement agreement.

Although the AG settlement mirrors the consumer settlement in many ways (*e.g.*, in requiring the hiring of a CISO, implementation of a written information security program, monitoring of information security events, and provision of security training to employees), the AG settlement is notable for the granularity of its technical requirements including:

- encryption;
- multi-factor authentication;
- whitelisting;
- network access controls;
- active log monitoring;
- segmentation of production and development environments; and
- enhanced access control measures for service, vendor, and administrator accounts.

LEARNING FROM TARGET'S SETTLEMENT

Companies should take note of the level of technical specificity in the settlement, as it may help define what AGs consider the appropriate baseline security protocols that companies should employ. In fact, in announcing the settlement, Illinois Attorney General Lisa Madigan stated that it "establishes industry standards for companies that process payment cards and maintain secure information about their customers."

The settlement stresses the need for an information security plan that fits the actual risks of the entity and its customers. This risk-based approach will be familiar from the NIST Cybersecurity Framework (among other standards), which continues to emerge as a *de facto* gold standard for cybersecurity assessments.

The settlement suggests entities:

- Conduct cybersecurity risk assessments.
- Implement a comprehensive information security program and incident response plan ("IRP").
- Stress test the information security program and IRP to ensure the policies and procedures are reasonable and appropriate given the entity's size, nature, and sensitivity of personal information maintained through, for instance, regular tabletop exercises.

These steps may help entities bolster their argument that they took reasonable measures to protect consumers' personal information, mitigating risk both by reducing the likelihood of a successful attack, and by positioning the company to succeed in regulatory investigations and private litigation.

This client update was originally issued on May 25, 2017.

Regulatory

"Does your car have any idea why my car pulled it over?"

Cybersecurity issues continue to be top of mind for regulators at every level and across every industry. Over the past year, several states have enacted new statutes governing cybersecurity, and a number of different regulators have issued new guidance to their regulated entities. This introduction will provide an overview of some of the key regulator efforts in this space that we are monitoring on a continuing basis.

On the whole, recent regulator activity has been characterized by an important shift: many regulators are putting out substantive

minimum requirements they expect every company—regardless of risk profile—to meet in order to demonstrate compliance. From maintaining up-to-date policies and procedures to implementation of entirely new practices, like two-factor authentication, companies are well advised to understand regulators' minimum expectations.

Financial and Insurance Industries. As more states adopt statutes with explicit cybersecurity requirements, financial entities will need to ensure that they have implemented comprehensive data security practices and are in compliance with specific regulatory requirements. One major area where we have seen a shift in substantive requirements in recent months is over vendor management.

For third party service providers, the New York Department of Financial Services ("DFS") Part 500 regulation requires entities to establish "relevant guidelines" addressing due diligence and/or contractual provisions covering topics such as the vendor's relevant policies and procedures, representations and warranties concerning those policies and procedures. The DFS regulations also contain one of the shortest timeframe notification obligations in the country: cybersecurity events must, under certain circumstances, be reported to DFS within 72 hours. The clock begins to run from a determination that a cybersecurity event either (i) must be reported to another government agency or regulator; or (ii) causes a "reasonable likelihood of materially harming" any material part of the normal operations of the company.

The Financial Industry Regulatory Authority ("FINRA") has also begun holding firms liable for cyber events at their third-party vendors, even when the firm itself is the victim of a breach. Financial institutions cannot escape liability by merely turning all of their

customer data over to a third-party. In FINRA's view (which is shared by DFS), policing the cybersecurity of vendors is a continuing responsibility for companies. To meet this obligation and upgrade vendor oversight, companies can include pre-engagement due diligence, enforce a rigorous program of access controls, and conduct ongoing testing and verification of vendor's security.

In October 2017, the National Association of Insurance Commissioners ("NAIC") adopted the Insurance Data Security Model Law. The NAIC Model Law requires companies to have an information security program, to know their cybersecurity risks via a risk assessment process, and to use appropriate controls to reduce these risks. Much of what would be mandated by the Model Law is widely regarded as best practice by the information security community. The law closely tracks the DFS regulation.

Retailers and the FTC. The U.S. Federal Trade Commission ("FTC") has continued to emphasize the need for companies to take appropriate measures to safeguard data security. For example, the FTC is making clear that it is not enough for companies active in the mobile space to ensure that applications are secure when released. Instead, the FTC expects companies offering mobile apps—or making mobile devices—to offer regular, transparent, and effective security updates to customers. Companies must be aware of new vulnerabilities, adapt their software to ensure that the software remains "reasonably" secure, and keep records of their security updates. Otherwise, they may be subject to violations of federal law including a finding that they engaged in deceptive conduct, or offered unreasonably weak security.

Given the rising incidence of cyberattacks and data breaches, the FTC is also sending a message that companies will be held

responsible for detecting events, and protecting their customers from attacks such as credential stuffing. Since most individuals reuse passwords and user names across websites, hackers can take advantage of this by accessing and testing out the credentials, and launching an invasion of user accounts across different websites. While there is no explicit legal mandate to detect and protect credential stuffing, in the FTC's recent investigation of TaxSlayer—which was the victim of a credential stuffing attack—the FTC brought an enforcement action on the premise that TaxSlayer violated the Gramm-Leach-Bliley Act's Safeguards Rule. This rule requires businesses to have a comprehensive written information security program, conduct security assessments which identify reasonably foreseeable internal and externals risks to the security, and implement safeguards to control the identified risks.

To protect customers from credential stuffing, the FTC has recommended that companies consider multi-factor authentication—for example, requiring the use of a password and separate code sent by different methods, such as an email or text. Notably, the DFS Part 500 regulations already require MFA for individuals accessing internal networks from outside.

Emerging Technologies. New technologies such as blockchain and the Internet of Things can pose significant risks to data privacy and security, and regulators are already active in these spaces. Industry attention to and the use of blockchain technology by firms has led FINRA to further the discussion around regulatory issues associated with its implementation. In a recent report about blockchain technologies in the securities industry, FINRA indicates that financial firms will need to ensure that they consider how to implement network security features, and adequately secure

customer data.[1] Firms will need to consider anti-money laundering, customer identification and "know-your-customer" requirements.

On January 27, 2015, the FTC issued a report on the Internet of Things ("IoT"), which refers to the ability of everyday objects to connect to the Internet and to send and receive data.[2] On its face, IoT has the potential to improve the lives of its many users. But with over 25 billion connected devices in use worldwide, the FTC report noted that these connected devices could significantly undermine consumer confidence by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety. The Report establishes a set of guidelines for businesses which includes building security into devices at the outset, and considering measures to keep unauthorized users from accessing a consumer's devices, data, or personal information stored on the network. Overall, though, it is unclear what regulatory framework specifically governs the Internet of Things. For now, the FTC has been focused on improving transparency and has started to launch enforcement cases against companies for failure to adequately inform and protect consumers' information collected through IoT devices.[3]

---

1 FINRA, *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry* (Jan. 2017), http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf.

2 *See* FED. TRADE COMM'N, *Internet of Things: Privacy & Security in a Connected World* (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

3 *See* FED. TRADE COMM'N, *D-Link Case Alleges Inadequate Internet of Things Security Practices* (Jan. 5, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/01/d-link-case-alleges-inadequate-internet-things-security.

Life Under the DFS Cybersecurity Regulations: One Year In

On March 1, 2017, the New York State Department of Financial Services ("DFS") Part 500 cybersecurity regulations (the "Regulations") came into effect. The first of their kind in the nation, the Regulations have brought many financial services companies into new territory. As companies get up to speed with the nuts and bolts of the Regulations, a number of common issues have emerged.

SCOPE

Financial services companies often have sophisticated, complex organizational structures—and these do not always fit neatly into the boxes created by the Regulations. The Regulations classify companies into four types: "Covered Entities" that must comply with the Regulation, "Affiliates" of Covered Entities that may not themselves be subject to the Regulations, "Third-Party Service Providers" of Covered Entities, and "Authorized Users" of a Covered Entity's information systems. For many companies, mapping out where related entities and individuals fall under the Regulations, how their information systems interact, and who should certify compliance to DFS, is not a simple exercise.

The key distinction for a company working through scoping questions to remember is entities that have access to the non-public information it holds and therefore affect its cybersecurity, are not necessarily entities that must independently comply with the Regulations. Company A, as a Covered Entity, may need to account in its risk assessment for risks posed by its affiliate Company B because they share servers—but that does not suddenly bring Company B, who is not licensed under any of the relevant New York laws, under the Regulations as well.

In the FAQs published by DFS, the best guidance available on the Regulations, DFS clarified the status of certain entities in the grey areas under the Regulations. Exempt mortgage servicers and New York branches of out-of-state domestic banks, for example, are not Covered Entities. But not-for-profit mortgage brokers, health maintenance organizations (HMOs), and continuing care retirement communities (CCRCs) are covered and need to comply with the Regulations.

EXEMPTIONS

Once it's settled if a company is a Covered Entity under the Regulations, the company might then consider if it—or any of its employees, agents, or representatives—qualifies for an exemption. Entities had until September 27, 2017, to file a notice of exemption for the certification deadline of February 15, 2018, but companies struggled with identifying who could be exempted and who could file exemptions on behalf of others.

DFS responded to this confusion and discussed various scenarios about the scope and logistics of exemptions in its FAQs. Certain Covered Entities can be pre-approved by DFS to file notices of exemption on behalf of their employees and captive agents under certain circumstances. Additionally, employees, agents, and representatives of another Covered Entity that are fully covered by that Covered Entity's cybersecurity program qualify for exemptions. In the event that circumstances change for the Covered Entity, it must file a new notice of exemption.

TRANSITIONAL PERIODS

Companies racing to get into compliance with the Regulations have also sought guidance on what exactly must be in place at the end of

each transitional period, and how that affects a company's certification of compliance. For example, a company may have identified the need for new access controls for Authorized Users through its risk assessment process, but be unable to fully implement those new controls by September 3, 2018. The Regulations are not clear on whether partial implementation of these controls would preclude certification of compliance on February 15, 2019.

DFS has not provided comprehensive guidance on this matter. In its FAQs, DFS addressed how companies should handle compliance with Section 500.05, which requires regular penetration testing and vulnerability assessments in the absence of continuous monitoring. DFS stated the company must have a plan in place that provides for appropriate penetration testing—but that the company need not have the first annual penetration testing and first vulnerability assessment completed by that time. Companies facing implementation challenges should keep tabs on the DFS FAQs and consider how to prioritize steps in a risk-based manner.

DILIGENCE

Under Section 500.09 and Section 500.11 of the Regulations, companies must account for changes to their operations and information systems. This responsibility includes performing due diligence and periodic assessments of the cybersecurity practices of their third-party service providers. But the Regulations left unclear how intensive the diligence must be, particularly where the third parties are themselves Covered Entities complying with the Regulations.

In its latest FAQs, DFS emphasized that companies need to conduct their own diligence and factual analysis of vendors they use and new companies they may acquire. It is not enough to take a third party's certificate of compliance at face value—companies must now "peek behind the curtain" to assess the cybersecurity programs of their vendors directly. Going forward, CISOs at Covered Entities should make an effort to get to know their counterparts at third-party vendors and begin building a long-term relationship. The more comfortable all sides are discussing their cybersecurity programs, the easier it will be to adapt to evolving cybersecurity threats in a coordinated fashion.

REPORTING CYBERSECURITY EVENTS

Section 500.17 of the Regulations requires companies to provide notice to the DFS Superintendent within 72 hours of determining that certain Cybersecurity Events have occurred. At first glance, there are two simple triggers for notifying DFS: when notice must be given to another government or self-regulatory body, or when the Cybersecurity Event is reasonably likely to materially harm a material part of the company's operations.

In practice, there is not much clarity on how broad the requirement is and how to provide notice through the new DFS cybersecurity portal. The Regulations, for example, do not specify whether notice to a foreign supervisory body triggers notice to DFS, or whether all cybersecurity-related suspicious activity reports to regulators like FinCEN must also be reported to DFS. Nor is it always obvious when unsuccessful attempts to gain unauthorized access to a company's network might be reasonably likely to materially harm a core aspect of the company's business. The one FAQ that DFS has published on the reporting requirements only made clear that DFS must be

notified after a data breach involving consumer harm—far from the trickiest question resulting from the notice provision.

Determining when to notify DFS ultimately depends on every company's own risk profile. Some companies have chosen to notify DFS when the lines are blurry, flagging that they are doing so out of an abundance of caution in these early days. Others have chosen to document internally their reasoning on why notice is unnecessary, based on their incident response plans and the facts they have.

Even when companies are sure that notice must be given, they remain uncertain about what that notice must look like. The DFS cybersecurity portal was created for the Regulations, and companies are not yet familiar with the interface or what information will be necessary to fulfill DFS' expectations for notice.

LOOKING AHEAD

Only months remain until the end of the final transition period for the Regulations, at which point companies must be fully compliant. The topics discussed above will become clearer as companies adjust to business under the Regulations and DFS provides additional FAQs and guidance. Compliance is clearly top of mind for DFS, which sent reminder emails to companies subject to the Regulations who did not submit certifications of compliance by February 15, 2018. Companies should expect DFS to remain keenly interested in monitoring compliance as March 1, 2019 approaches.

In the meantime, companies should recognize they are not alone in navigating the Regulations. Maintaining a dialogue with peers in the industry and with outside counsel can be an effective way of staying

up to date with best practices as the end of the transition period approaches.

NAIC Insurance Data Security Model Law

On October 24, 2017, the National Association of Insurance Commissioners ("NAIC") formally adopted the final draft of its Insurance Data Security Model Law (the "Model Law"). In May 2018, South Carolina became the first state to enact legislation tracking the Model Law. Other states may well follow suit.

The NAIC Model Law is another indicator that regulators and legislators, while encouraging a risk-based approach to corporate cybersecurity, will not hesitate to impose certain minimum requirements companies must meet or be considered legally noncompliant.

FEATURES OF THE NAIC MODEL LAW

The Model Law is designed to complement whatever pre-existing data privacy and consumer breach notification obligations might already be in place in states that adopt the Model Law. The Model Law can be modified as needed, or adopted in its entirety. Its core requirements, as described below, include the obligation to implement a written Information Security Program. All insurance companies licensed to do business in adopting states would be subject to the provisions of the Model Law, with only narrow exemptions to compliance.

Employees and agents of a licensee who are themselves licensees would not be required to develop an Information Security Program, so long as they are covered by their own organization's program. Licensees with fewer than ten employees, including independent contractors, are also exempt from the Information Security Program requirements. Licensees under the Health Insurance Portability and Accountability Act ("HIPAA") are exempt from Information

Security Program requirements provided they able to certify compliance with HIPAA's Information Security Program requirements.

Substantive Requirements

The Model Law imposes a set of requirements on licensees, including that they:

- Conduct risk assessments no less than annually to determine the likelihood and potential damage of reasonably foreseeable internal or external threats;
- Implement a written Information Security Program that reflects the size and complexity of the licensee, as well as the nature and scope of the licensee's activities and the sensitivity of the nonpublic information utilized by the licensee or in the licensee's possession based on the licensee's risk assessment;
- Develop of a written incident response plan designed to promptly respond to and recover from cybersecurity compromises; and
- Report to the board on at least an annual basis regarding the overall status of the Information Security Program and the licensee's compliance with the Model Law as well as material matters related to the Information Security Program.

Information Security Program

The Model Law mandates that licensed entities have an Information Security Program that details the administrative, technical and physical safeguards that a licensee uses to access, collect, distribute, process, store, use, transmit, dispose of, or otherwise handle nonpublic information. Insurers will be required to submit annually, to their domiciliary state's insurance commissioner, a certification confirming their compliance with the Information Security Program provision of the Model Law.

ADOPTION

The recently issued New York State Department of Financial Services ("NYDFS") regulation, 23 NYCRR 500, in many ways appears to have served as a template for NAIC. Notably, the Model Law is applicable only to insurance licensees, whereas the NYDFS regulation applies to all financial services companies regulated and licensed by NYDFS—meaning banks are covered too. A drafter's note from NAIC specifies that the intent is for companies in compliance with the NYDFS regulation to be deemed compliant with the Model Law.

South Carolina

The South Carolina legislature was the first in the nation to enact the Model Law into actual state law. Its version includes all of the hallmark features of the Model Law, including an information security program based on the licensee's risk assessment, required risk assessments, the implementation of various safeguards and annual assessment of the safeguard's key controls, systems and procedures, an incident response plan and board involvement via annual cybersecurity briefings.

Licensees have until July 1, 2019 to implement their Information Security Programs and to establish an incident response plan and until July 1, 2020 to have a third-party service provider management system in place.[1]

Rhode Island

Rhode Island has two pending bills adopting the Model Law which are currently in committee. The two bills are House Bill No. 7789

[1] South Carolina Insurance Data Security Act, https://www.scstatehouse.gov/sess122_2017-2018/bills/4655.htm.

and Senate Bill No. 2497. House bill No. 7889 was introduced on February 28, 2018. Senate bill No. 2497 was introduced on March 1, 2018. Both bills are currently on hold for further study.

Both bills appear to adopt the Model Law with little modification. Both include a mandatory incident response plan, risk assessment, annual reporting (at a minimum) to the board of directors, and the management of risk via appropriate safeguards. Both bills provide that the requirements would take immediate effect.

CONCLUSION

The NAIC Model Law and the DFS regulation reflect the emerging trend toward combining a risk-based approach to cybersecurity regulation with a specific and prescriptive approach. Companies across jurisdictions should therefore be prepared to develop and implement such approaches going forward.

LabMD Beats FTC in Cybersecurity Appeal – What's Next for "Reasonableness"-Based Enforcement Cases?

One of the longest-running legal sagas in cybersecurity has ended, at least for now: the Eleventh Circuit Court of Appeals rejected the Federal Trade Commission's ("FTC") cease and desist order requiring LabMD to implement "reasonable" cybersecurity practices because it lacked the necessary specificity to permit court enforcement. The decision takes a scalpel to the FTC's cybersecurity authority, but not the ax that some had expected. It portends modest yet meaningful limits on the FTC's enforcement authority both in cybersecurity and, potentially, in other areas such as false advertising.

What happened? The case dates back to 2005, when a LabMD billing manager installed a peer-to-peer file-sharing application on her work computer, inadvertently making some medical records available online. The FTC challenged LabMD's allegedly poor cybersecurity practices as unfair in violation of Section 5 of the Federal Trade Commission Act ("FTC Act").

LabMD proved to be the unusual company that fought the FTC rather than settling. At the agency level, the FTC imposed a cease and desist order requiring LabMD to have "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." LabMD appealed.

In an interim ruling in 2016, the Eleventh Circuit stayed the FTC order—questioning whether, as a matter of law, any unfair business practice could occur without better proof of consumer harm. (The patient records were exposed, but the FTC lacked evidence of actual

misuse.) In the final ruling, the Eleventh Circuit vacated the FTC order because "it does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data security program and says precious little about how this is to be accomplished."

Notably, the Eleventh Circuit stated that the *prohibitions* contained in an FTC cease and desist order must be specific—stated with clarity and precision. The LabMD order did not contain any prohibitions, only general directives to implement reasonable cybersecurity practices. The Court found that these order provisions were too ambiguous and therefore unenforceable.

Key Takeaways. After this long-awaited decision, what has changed and what has not?

- The FTC's basic authority to bring enforcement actions for "unreasonably" lax data security practices under the unfairness prong of Section 5 remains debatable but was not overturned by the Eleventh Circuit. This authority was specifically affirmed by the Third Circuit in the much-discussed Wyndham Hotels case. The Eleventh Circuit here sidestepped the issue. Rather, it assumed the FTC has authority to deem unreasonably poor security an unfair business practice, and instead focused on limitations associated with the FTC's injunctive remedies.
- Likewise, the court chose not to adopt a stringent requirement of substantial actual harm, which had been suggested in the interim decision. Proof of actual harm is often hard to come by in data breaches. Such a requirement thus would sharply reduce the number of cases in which the FTC could invoke its unfairness authority.
- For companies confronting a particular FTC enforcement action based upon a data breach or cybersecurity practices, there is now a

clear new limit on remedies: the injunctive provisions in future FTC orders (whether imposed by the Commission or a court, or agreed to by settlement) will have to be more detailed about what amounts to "reasonable" security. Orders may also have to be more closely tied to the particular security practices at issue in a given case and may need to be drafted as "prohibitions." Time will tell how much detail, and how close a tie, are needed to pass legal muster. Many companies are under existing FTC settlement orders—most of which include similar requirements and many of which are applicable for periods up to 20 years (or longer). In the event that the FTC alleges that a company has violated one of these orders, that company may now have a basis to argue that portions of the order are unenforceable.

- Companies facing FTC false advertising challenges may also be able to use the *LabMD* decision to their benefit. When the FTC resolves a case based on allegedly false advertising, its orders frequently require a "reasonable basis" and "competent and reliable scientific evidence" in support of future claims. Arguably, that approach has many of the same weaknesses identified by the Eleventh Circuit related to ambiguity and lack of precision. The FTC may contend that its approach in advertising cases is more defensible because the meaning of these terms has become well settled across decades of enforcement matters. A "reasonableness" standard in cybersecurity is both newer and arguably more dynamic, and therefore harder for a court to enforce. Thus, it is uncertain whether the Eleventh Circuit *LabMD* decision will limit the FTC's remedial authority outside the cybersecurity realm.
- "Reasonable" security remains the basic legal standard for planning or assessing a corporate cybersecurity program. The Eleventh Circuit avoided a frontal attack on the reasonableness standard, and more than a dozen states, notably including

> California, have enacted laws that require "reasonable" cybersecurity. Like the FTC, these state legislatures have not decreed specific benchmarks for what is reasonable (though California's attorney general has pointed to the Center for Internet Security's 20 Critical Security Controls.) Some courts also have let negligence-based challenges survive motions to dismiss in post-breach class action lawsuits.

Companies seeking legal compliance thus are still well-advised to adjust their cybersecurity practices, evaluating the latest best-practice responses and adopting them in a risk-based manner as the threat landscape evolves.

This client update was originally issued on June 26, 2018.

New FTC Guidance for Security Updates to Mobile Devices and Applications

A new report from the Federal Trade Commission emphasizes that companies offering mobile apps—or making mobile devices—should offer regular, transparent, and effective security updates to consumers. Companies failing to do so risk a finding that they engaged in deceptive conduct, or offered unreasonably weak security, in violation of federal law.

The FTC noted that:

- Security should be part of the design process, including as products are updated. Updates should be provided for a time period consistent with consumer expectations, and companies should track when and how they issue updates—and whether consumers actually install them.
- Security updates should be treated differently from general software updates and provided separately when appropriate.
- Companies should be transparent with consumers about the importance of updates, the minimum support period for devices and applications, and when devices or software are out of date. Industry groups should work with the government and advocacy groups to promote consumer education about the importance of security updates.

This FTC report is likely a step toward future enforcement action against companies that do not live up to this guidance. As the FTC argued—and the Third Circuit upheld—in the *Wyndham* litigation, the FTC may use guidance documents and public statements to develop a substantive body of rules that put companies on fair notice of what data security practices would be so weak as to constitute an unfair business practice in violation of Section 5 of the FTC Act.

The FTC is making clear that it is not enough for companies to ensure that applications are secure when released. The cybersecurity threat landscape is ever-evolving, and companies must be aware of and adapt their software to new vulnerabilities—from the recent discovery of the Meltdown/Spectre design flaw to new types of dangers, like the growing trend toward enterprise-level ransomware attacks.

Looking ahead, the report indicates a few areas of focus for companies active in the mobile space:

- It's not enough to release an app and forget about it—companies should be constantly working to ensure that the app remains reasonably secure.
- The FTC is concerned with how companies build and deploy security updates, highlighting how security is different from other steps in design and development. The FTC recommends "security-only updates"—that is, not waiting to deploy patches until new app features are also ready—and a streamlined update process.
- The FTC's report also puts the onus on companies to monitor how consumers respond to their security updates—meaning that just releasing a security update may not be enough. Significantly, the FTC is encouraging companies to keep records about their security updates and consumer adoption, and learn from their past practices. It's possible that, down the road, the FTC might look to whether companies are doing enough to ensure that their customers actually adopt security updates.

This client update was originally issued on March 7, 2018.

Cybersecurity Enforcers Wake Up to Unauthorized Computer Access Via Credential Stuffing

Do you ever use the same username and password on more than one website? Most people sometimes do, and thereby put themselves at risk for "credential stuffing." That's what it's called when hackers take usernames and passwords that were compromised in a past breach of Site A, and use them to launch a new invasion of user accounts on Site B.

Now the U.S. Federal Trade Commission has brought its first-ever enforcement case in this area. The target? Not a hacker, but TaxSlayer LLC, aka Site B. TaxSlayer is an online tax preparation service that fell victim to a credential-stuffing attack.

The FTC's message is loud and clear: If customer data was put at risk by credential stuffing, then being the innocent corporate victim is no defense to an enforcement case. Rather, in the FTC's view companies holding sensitive customer information should be taking affirmative action to reduce the risk of credential stuffing. In particular, the TaxSlayer case strengthens a trend toward making multi-factor authentication—the use of a second layer of entry credentials, like a text message code, in addition to a password—all but a legal requirement for financial institutions.

HOW CREDENTIAL STUFFING WORKS

Let's say Harry Hacker breaks into the network of OnlineRetailer.com. Once in, Harry obtains a million customers' username and password combinations. Jane Jones, for example, accesses OnlineRetailer.com with the username

"janejones@gmail.com" and the password "janespassword". And now Harry Hacker knows it.

Next Harry begins to look for other websites to attack. Or, perhaps, he markets the stolen credentials on the "dark web"—the shadowy corner of the Internet where bad guys traffic in black-market data. Those username-and-password combinations that Jane Jones and a million others use at OnlineRetailer.com are now circulating among cybercriminals.

Next, Harry Hacker (or Hacker #2, having bought the compromised credentials on the dark web) launches a new round of attacks. He takes all those stolen credentials from OnlineRetailer.com, and uses an automated tool to enter the credentials en masse at OnlineBank.com, OnlineBroker.com, and OnlineTravel.com. Jane Jones uses the same username and password at all four sites. The hacker now has access to her accounts at all four. That includes access to her credit card numbers, account numbers, and other personal details Jane has stored there for convenience.

Notably, the hacker has not gained general access to any of these companies' networks. Nor do any of the companies involved necessarily even have any clue that the attacks are even happening. On the contrary, to them, it simply looks like Jane Jones—a known user—has entered her legitimate credentials.

Credential stuffers are taking advantage of two unhappy trends. First, upwards of 80% of people are estimated to reuse credentials across at least some of their online accounts. Second, as more companies fall victim to data breaches, the pool of compromised

credentials gets bigger. The upshot is that with each new breach, credential-stuffing attacks may become exponentially more effective. Published reports indicate that high-profile companies, such as Pinterest Inc., and Groupon Inc., are among the many that have suffered credential-stuffing attacks.

THE TAXSLAYER INVESTIGATION AND SETTLEMENT

As with many FTC enforcement matters, the TaxSlayer complaint and settlement (in the form of a consent order) were publicly released on the same day. The publicly available "facts" therefore are as set forth by the FTC in its rather bare-bones pleading.

The complaint explains that TaxSlayer operated a browser-based and mobile tax return service. Users were required to create accounts and to input a slew of personal information. TaxSlayer therefore found itself holding details about its customers ranging from their Social Security numbers to their bank account and credit card numbers to their marital status, dependents, financial assets, and health insurance.

From Oct. 10 to Dec. 21, 2015, TaxSlayer suffered a credential-stuffing attack. (The FTC actually uses the less fun term "list validation attack.") The cybercriminals were able to access nearly 9,000 TaxSlayer customers' accounts. The bad guys filed an unknown number of fraudulent returns, directing refunds to themselves instead of to the actual taxpayers. The attack ended when TaxSlayer imposed a multifactor authentication requirement. The FTC specifically notes that TaxSlayer was unaware of the attack until it received a user complaint in January 2016. The complaint itemizes a

long list of harms suffered by consumers whose tax accounts are compromised.

The legal challenge for the FTC was that no applicable statute, regulation or caselaw specifically imposed any duty on TaxSlayer to detect or prevent credential stuffing. The FTC relied instead on a more general theory: namely, that TaxSlayer had failed to meet the Privacy Rule and the Safeguards Rule of the Gramm–Leach–Bliley Act (GLBA). The GLBA is a data privacy statute that applies to "financial institutions," meaning all businesses that are "significantly engaged" in "financial activities." A company may meet this definition even if "financial activities" are not its primary purpose. For example, a car dealership offering car loans may be covered. While TaxSlayer lacked the traditional trappings of, say, a bank or an investment adviser, the FTC contended that its tax return activities made it subject to the GLBA.

The Privacy Rule requires institutions subject to the GLBA to provide their customers with a notice explaining the company's privacy policies and practices. An accompanying rule, "Reg P," requires that the notices be delivered in a way that consumers are reasonably expected to receive them. Because privacy policy links on homepages are deemed insufficient by the FTC, this often results in physical notices being mailed to consumers annually. You may know this as the piece of paper from your bank that you annually recycle without reading.

The FTC alleged that TaxSlayer "failed to provide a clear and conspicuous initial privacy notice" and "failed to deliver the initial privacy notice so that each customer could reasonably be expected to

receive actual notice" in violation of the Privacy Rule and Reg P. One might ask—so what? Compliance with the Privacy Rule or Reg P is certainly an important legal mandate, but here it would not have stopped the credential-stuffing attack.

The Safeguards Rule has more teeth, and here's where TaxSlayer perhaps felt more bite. This rule requires covered institutions to have a "comprehensive written information security program." Companies are required to conduct security assessments and "design and implement information safeguards to control the risks" identified during those assessments. § 314.4(c). TaxSlayer was alleged to be in violation of this rule because it "failed to have a written information security program until November 2015," and "failed to conduct a risk assessment, which would have identified reasonably foreseeable internal and external risks to the security."

Notably, the FTC alleged that credential-stuffing attacks have become reasonably foreseeable. On that hook, the FTC essentially hung a legal mandate to detect and prevent such attacks—translating the general requirements of the Safeguards Rule into a de facto set of highly specific requirements. The FTC ticked off a list of alleged failures by TaxSlayer that the complaint said violated the Safeguards Rule:

- A weak password requirement, the only mandate being that the password be 8 to 16 characters.
- A lack of "risk-based authentication methods," *e.g.*, multi-factor authentication. As noted, this is when, for example, your bank texts you a temporary access code which you must enter to get to your account online, the code changing every time you log in.

- Not telling customers when someone had made a material change to their address, password or security question.
- Not validating email addresses at account creation.
- Not using "readily-available tools" to prevent attempted credential stuffing. The FTC didn't say what tools it had in mind, but security experts promote the use of several, such as IP blacklisting—a tool that spots and blocks any IP address attempting to generate a large number of login attempts in a short period of time.

Each of these steps would certainly be endorsed by security experts as a best practice for many companies in many contexts. The TaxSlayer case highlights that the FTC effectively regards these best practices as having the force of law. Put another way: any financial institution that is covered by GLBA, holds sensitive customer information, and is not utilizing these tools may face an uphill battle if they suffer a future credential-stuffing attack and the FTC comes calling.

The FTC's press release accompanying the settlement strongly suggested that, among these now de facto requirements, multi-factor authentication is first among equals. Tom Pahl, acting director of the FTC's Bureau of Consumer Protection, said the case "demonstrates the importance of password protection … Hackers took advantage of people who re-used passwords from other sites, and the attack ended when TaxSlayer eventually required people to use multi-factor authentication." (emphasis added). The FTC published a blog post about the case entitled "TaxSlayer: File this one under authentication."

The consent order agreed to by TaxSlayer bolstered the FTC's position in a number of ways. TaxSlayer was placed under a 20-year requirement to conduct risk assessments, tailor its information security program to the results, and certify the effectiveness of its information security program. TaxSlayer specifically undertook to comply with GLBA, including the Privacy Rule and the Safeguards Rule. While this legal requirement would apply in the absence of a consent order, the order subjects TaxSlayer to contempt risk if it does not comply with the law. The words "multi-factor authentication" are not found in the consent order, but they might as well be. TaxSlayer must comply with the Safeguards Rule, and the FTC clearly regards multi-factor authentication as part of that compliance obligation.

HOW MULTI-FACTOR AUTHENTICATION DETERS CREDENTIAL STUFFING

There are many ways that companies might prevent or limit credential-stuffing attacks on their platforms. For example, as suggested by the FTC's ticklist in the TaxSlayer complaint, companies can:

- Ask an additional security question when a user logs in from a new device.
- Require strong, complex passwords and make users change them at regular intervals—reducing the odds that the user will adopt the same credentials across multiple sites.
- Limit the number of unsuccessful log-in attempts from a particular device or IP address within a given time window. (Note that clever criminals may be able to pace their automated attacks to defeat such limits.)

- Require manual entry of additional information, such as the last four digits of a previously obtained credit card or Social Security number, prior to major actions such as purchases or submitting tax returns.

Among these, the FTC has chosen to highlight multi-factor authentication. Multi-factor authentication is the process by which the user's identity is verified by drawing on the functionality of another device. As noted, this often takes the form of a temporary code being sent to a second device. The user then enters this code to log into the platform. The code can be delivered via text message or draw upon software designed for the purpose, such as RSA Security LLC's SecureID. Other forms exist as well. For example, a flash drive might serve as a key, only allowing a log-in for that user from devices with the flash drive inserted.

The principal feature of multi-factor authentication is that, in order for the user to log in or to perform certain sensitive functions, the user must have access to a device or application separate and apart from the relevant platform. This prevents cybercriminals from accessing a user's account even if they possess the correct initial login credentials.

The TaxSlayer settlement is not the first time the FTC has beaten the drum for multi-factor authentication. In April 2016, the FTC published "*Mobile Health App Developers: FTC Best Practices*." The FTC recommended that developers consider authentication carefully when designing an application: "If risks are substantial, consider multi-factor authentication—for example, requiring the use of a password and a separate code sent via another channel, such as an

email or text." In June of 2016, the FTC issued a guide targeted to consumers addressing what to do in the event of a password breach. The first recommendation: "use multi-factor authentication, when it's available."

Later in 2016, the FTC expanded its more targeted recommendations to businesses generally. When issuing the 2016 update to its "*Protecting Personal Information: A Guide for Business*," the FTC added recommendations on using multi-factor authentication and noted that a key point in the revised guide was that developers should "consider using multi-factor authentication, such as requiring the use of a password and a code sent by different methods." A post on the FTC's business blog in August 2017 reiterated: "to combat credential-stuffing attacks and other online assaults, companies should combine multiple authentication techniques for accounts with access to sensitive data." (emphasis added).

The first FTC investigation and settlement in which the FTC clearly labeled the lack of multi-factor authentication an issue was announced on Aug. 15, 2017. The FTC alleged inappropriate data handling practices at the ridesharing company Uber Technologies Inc.—both undue access to riders' personal data by Uber's own employees and an external breach facilitated by an Uber employee publicly posting the login key online. The focus of the accompanying press release was on the lack of measures taken to ensure rider data security. The FTC noted: "Uber did not require engineers and programmers to use distinct access keys to access personal information stored in the cloud. Instead, Uber allowed them to use a single key that gave them full administrative access to

all the data, and did not require multi-factor authentication for accessing the data." (emphasis added).

While the Uber settlement itself did not explicitly call for the implementation of multi-factor authentication, the accompanying FTC press release noted multi-factor authentication is an effective privacy protection tool. The settlement agreement broadly directed Uber to initiate "the design and implementation of reasonable controls and procedures to address such risks and regular testing or monitoring of the effectiveness of those controls and procedures." The Uber case makes clear that multi-factor authentication may be seen as required not just for external access, but as part of a company's internal access controls as well.

The trend toward multi-factor authentication has been strongly reinforced at the state level. Last year, New York's Department of Financial Services adopted a first-in-the-nation cybersecurity regulation applicable to "Covered Entities"—banks, insurance companies and other firms licensed by DFS, which is to say thousands of the largest financial institutions in the country and the world. Over time, Covered Entities must implement multi-factor authentication "for any individual accessing the Covered Entity's internal networks from an external network," unless the chief information security officer specifically approves the use of "reasonably equivalent or more secure controls." More generally, Covered Entities are required to use "effective controls"—which, DFS specifically notes, "may include Multifactor Authentication"—to "protect against unauthorized access" to information and systems. 23 NYCRR § 500.12.

CONCLUSION

TaxSlayer is the first word from the enforcement community on credential stuffing, and not the last. It remains the case that there is no explicit legal mandate to prevent and detect credential stuffing, whether under the name "list validation attacks" or any other. Companies whose conduct in this area is called into question will always have case-specific defenses to offer as to why their cybersecurity program, as a whole, was reasonably configured to deal with foreseeable risks.

Nonetheless, if it wasn't clear before, it is after TaxSlayer: Companies that fail to consider the risks of credential stuffing, and to implement mitigating controls, do so at their peril. Companies that fail to use multi-factor authentication to protect sensitive data do so at their particular peril. The precise legal hook relied upon by privacy enforcers will always vary from case to case, but the enforcement community's commitment to these principles is here to stay.

This article originally appeared in Bloomberg Law: Big Law Business on February 20, 2018.

NY Cybersecurity Bill Shows "Reasonable Security" Standard Gathering Force

On November 1, 2017, New York Attorney General Eric Schneiderman announced a proposed bill called the Stop Hacks and Improve Electronic Data Security ("SHIELD") Act. The SHIELD Act would broaden New York's breach disclosure requirements. It also would require that all businesses, breached or not, adopt "reasonable" cybersecurity measures. Reasonable security has been steadily gaining traction as a legal standard both in the United States and globally. Whether or not the SHIELD Act becomes law, its introduction is a prompt to ask whether your cybersecurity program is "reasonable."

HOW WOULD THE SHIELD ACT CHANGE NEW YORK LAW?

- Entities failing to adopt "reasonable" security measures, or failing to notify affected consumers after a data breach, would be subject to an enforcement action by the New York Attorney General.
- Entities holding personal information of New York residents would be subject to New York's law, even if they do not do business in New York.
- New categories of information would be added that, if breached, would trigger disclosure requirements: username and password combinations, biometric information, and health information covered by the federal Health Insurance Portability and Accountability Act.
- There would be a safe harbor against New York AG enforcement actions for entities that have "reasonable" cybersecurity, as certified by an independent organization (such as the National Institute of Standards and Technology ("NIST")), or by compliance with specific requirements outlined in the proposed statute.

WHAT IS "REASONABLE" SECURITY?

The SHIELD Act joins a growing U.S. and international legal trend toward imposing substantive cybersecurity standards, not just breach notification requirements.

- The U.S. Federal Trade Commission has brought numerous enforcement actions against breached companies. The legal hook is that less-than-"reasonable" security allegedly amounts to an unfair business practice under Section 5 of the FTC Act. An FTC blog launched in July distills these cases into a list of what the FTC considers reasonable security measures.
- The U.S. Securities and Exchange Commission has made clear that it expects broker-dealers and investment managers to have a comprehensive cybersecurity program in place.
- New York's Department of Financial Services has spelled out comprehensive, specific cybersecurity requirements for banks and insurance companies licensed in New York.
- U.S. federal courts have allowed common-law negligence claims to survive motions to dismiss in recent cases arising from the data breaches at Target, Sony, and The Home Depot. The essence of a negligence claim, of course, is that the company has a duty to maintain reasonable cybersecurity in the first place.
- Over a dozen U.S. states, including California, Florida, Nevada, and Texas, already have statutes requiring "reasonable" cybersecurity. California's Attorney General has opined that compliance with the California statute requires compliance with the Center for Internet Security's Critical Security Controls.
- The European Union's General Data Protection Regulation ("GDPR"), which takes effect in May 2018, requires businesses to have "appropriate technical and organisational measures to ensure a level of security appropriate to the risk"—essentially a

> reasonable security requirement by a different name. The GDPR sets out a non-exhaustive list of "appropriate" measures, including pseudonymization and encryption of personal data as well as "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures."

By definition, "reasonable" security is a moving target. As security best practices become broadly accepted in the technical community, they morph into legal requirements. What's reasonable today may not be reasonable tomorrow. The SHIELD Act is a useful snapshot of what the New York Attorney General considers reasonable right now:

- An internal cybersecurity program, run by employees designated to deal with data security, that identifies risks, assesses safeguards, trains employees in security procedures, contractually requires vendors to maintain appropriate safeguards themselves, and adjusts to changed circumstances;
- Regularly tested technical safeguards that assess network risks and can prevent, detect, and respond to attacks or system failures; and
- Physical safeguards that protect against unauthorized access to private information, together with policies and procedures that assess risks in information storage and disposal, and dispose of private information once it is no longer needed for business purposes.

The SHIELD Act also considers compliance with NIST Special Publication 800-53 or the International Standards Organization (ISO) Standard 27002 to be evidence of reasonable security. Both NIST and ISO require businesses to be proactive in maintaining a

data security program that includes technical and physical safeguards, and to continually assess risks so that safeguards can be updated.

WILL THE SHIELD ACT BECOME LAW—AND IF NOT, WHY CARE?

New York is notorious for passing legislation only when it is engineered by "three men in a room"—the Governor, Assembly Speaker, and State Senate Majority Leader. Observers will note that the Attorney General is not one of the three. Attorney General Schneiderman proposed legislation similar to the SHIELD Act in 2015. It did not become law.

Even if the SHIELD Act does not become law, it matters. Like the FTC, the New York Attorney General regularly brings enforcement cases on the premise that the hacked company's pre-breach security was not reasonable. (Hilton paid $700,000 in settlement to the AG just last week.) When the AG's office lays out its view of what constitutes reasonable security, that is a good roadmap for possibly avoiding enforcement action in New York.

The SHIELD Act promises to be a useful guidepost nationally and globally as well. Its standards closely resemble those of the FTC, the GDPR, existing laws in other U.S. states, and other sources of legal guidance on reasonable cybersecurity. Companies engaged in "legal health checks"—that is, comparing their own cybersecurity to current best practices and legal requirements, and then moving to close any gaps—will therefore be well advised to look closely at AG Schneiderman's proposal.

This client update was originally issued on November 7, 2017.

Executive Order on Cybersecurity Raises More Questions than It Answers

On May 11, 2017, President Trump signed an executive order ("the Order")[1] designed to strengthen the cybersecurity of federal networks and critical national infrastructure ("CNI"), such as emergency services, energy and water systems, the communications sector, financial services firms and the Defense Industrial Base.[2] The stated purpose of the Order, initially announced in January, is to enhance U.S. federal and critical infrastructure information technology systems to protect and better serve the American people. In practice, the Order does not implement any immediate changes to U.S. cybersecurity policy but instead orders a series of sweeping reports to the President as one step in enhancing the cybersecurity of federal agencies and CNI.

THE EXECUTIVE ORDER SEEKS TO STRENGTHEN FEDERAL, CNI AND NATIONWIDE CYBERSECURITY

The Order requires that agency heads produce cybersecurity risk assessments addressing three groups: federal agencies, CNI entities and the U.S. workforce at large. First, the Order proposes strengthening federal networks by holding department and agency heads directly accountable for risk mitigation within their respective departments or agencies. This requires department or agency heads to provide an assessment of potential threats and correlating risk models. The Order mandates that agencies follow the National

1 The White House, Office of the Press Secretary, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017), https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

2 *See* 42 U.S.C. § 5195c(e); Exec. Order No. 13636, 78 FR 11739 (Feb. 12, 2013).

Institute of Standards and Technology ("NIST") Cybersecurity Framework[3] when creating their risk mitigation strategies. In addition, the Order seeks to modernize the federal architecture by establishing a preference for shared IT services within the executive branch such as email and cloud services.

Second, the Order requires that agency heads engage with the owners and operators of CNI to determine how the executive branch can support CNI entities in their own cybersecurity risk management efforts. Specifically, agency heads are to solicit the input of CNI entities deemed to be at the greatest risk of attack in order to determine which agency authorities and capabilities can best be leveraged to mitigate risks and defend against attacks. The Order specifically highlights concerns regarding resiliency against botnets or distributed denial of service ("DDoS") attacks, potential distribution of the electrical grid and risks faced by military or defense industrial systems.

Finally, the Order concludes by highlighting the need to create an efficient, reliable and secure U.S. internet space that respects privacy and protects against fraud or theft. This final section also requires that agency heads create additional reports for the president identifying international cybersecurity priorities and means of developing a more robust cybersecurity workforce through education and training.

---

[3] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (Feb 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

IMPLICATIONS FOR COMPANIES

There are several takeaways for private companies.

First, the Order's mandate that federal agencies align with NIST signals a continued hardening of the nominally "voluntary" framework into a de facto gold standard for cybersecurity assessments.

Second, the Order's direction that federal agencies implement "risk management measures commensurate with the risk and magnitude of the harm" posed by cyberattacks echoes regulators' calls for businesses to take a risk-based approach to managing cybersecurity. Businesses can expect the "risk-based" model to continue to gain acceptance, demanding an enterprise-wide view of cybersecurity risks and mitigation strategies.

Finally, the call for public/private cooperation (both domestically and internationally) may signal continued willingness by the government to share threat information in a two-way dialogue with industry, potentially increasing the benefits of engaging with law enforcement in the event of a cyber attack.

Overall, though, the Order raises more questions than it answers for the private sector as it does not explicitly call for new regulations specifying what companies must do to protect and defend their networks. Whether the reports to be provided to the president will

result in legislation or regulations more directly impacting cybersecurity in the private sector remains to be seen.[4]

This client update was originally issued on May 17, 2017.

[4] The authors would like to thank HJ Brehmer, a Summer Associate at Debevoise & Plimpton, for her assistance with and contributions to this client update.

The Future of Blockchain: FINRA Has Some Thoughts

Given the broad scope of possibilities inherent in distributed ledger ("Blockchain") technology, many firms in the securities industry have been eager to explore how to adopt and apply the technology to their businesses. The industry's attention to Blockchain has led the Financial Industry Regulatory Authority ("FINRA") to release a report examining the potential impacts of the technology on the business and regulation of the securities industry (the "Report").[1] In conjunction with the release of the Report, FINRA has requested that interested parties send comments concerning any aspect of the paper by March 31, 2017.

The Report provides a good overview of Blockchain technology, how it might be applied in various aspects of the securities industry and some of FINRA's thoughts on regulation of this new technology. FINRA adopts a cautiously optimistic tone towards the use of Blockchain. The use of Blockchain by firms may also be a means for regulators to further their own mission of protecting investors, although this point is not addressed by the Report.

BACKGROUND

Blockchain allows transactions to be recorded on a decentralized database maintained through a peer-to-peer network (the so-called distributed ledger). A transaction is initiated by any member of that network and is then verified by the other members. Once verified, the transaction is "cryptographically hashed" and permanently

[1] FINRA, Distributed Ledger Technology: Implications of Blockchain for the Securities Industry (Jan. 2017), *available at* http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf.

recorded on the distributed ledger. The recording is then secured with a private key and, in general, once set it cannot be altered.

Blockchain technology has many potential applications for the securities industry, including for broker-dealers. For example, FINRA notes that firms currently are examining the use of the technology to execute, clear and settle securities trades, syndicated loans and credit default swaps. In addition, firms are exploring the use of Blockchain to standardize reference data for certain securities products, create a centralized client identity management function, and to streamline certain procedures related to industry-wide utilities. The Report briefly discusses various other possibilities but does not mention any applications directly associated with the Consolidated Audit Trail.

REGULATORY CONCERNS

In the Report, FINRA identifies a number of areas in which Blockchain may introduce additional regulatory uncertainty into the securities industry. FINRA appears to view Blockchain as having the potential to create a "paradigm shift" for broker-dealers, and thus it believes that many areas may require additional attention from both the industry and regulators. For example, the Report indicates that firms will need to ensure that the uses of Blockchain comport with the relevant supervision requirements. Furthermore, and of paramount importance, the Report asks firms to appropriately consider how to implement network security features, particularly where customer data is implicated.

In addition, the Report notes that firms also will need to take into consideration anti-money laundering, customer identification and "know-your-customer" requirements. The Report indicates that

firms can take these steps by, among other means, determining how to verify the identities of parties with whom it transacts on the Blockchain network and by considering how to engage in transaction monitoring in accordance with the firm's existing anti-money laundering processes.

In considering the various applications for Blockchain, the Report notes its possible uses for tracking transfers of private company shares and facilitating faster clearing and settlement of transactions in securities, syndicated loans and other asset classes, as well as other "industry utility" functions to streamline repetitive processes. On this basis, FINRA indicates that broker-dealers using Blockchain technologies should consider the implications under the financial responsibility rules (SEC Rule 15c3-1 and 15c3-3), FINRA Rule 4311 relating to carrying agreements and transaction monitoring/surveillance requirements such as the market access rule (SEC Rule 15c3-5). Finally, FINRA states that broker-dealers must ensure that the information recorded on the Blockchain complies with recordkeeping rules under SEC Rules 17a-3 and 17a-4 and FINRA Rule 4511.

BENEFITS AND RISKS

According to the Report, Blockchain technologies have two primary potential benefits: (1) transparency by making available the complete history of all securities transaction on one network, and (2) improved market efficiency through eliminating many post-transaction processes.

The Report, however, raises a number of security, operational and governance concerns regarding the implementation of Blockchains. Unlike Bitcoin, Blockchains used by financial firms will most likely

run on a private network with a central governing body. Market participants will need to determine how such a network will be governed and managed. They also must establish eligibility criteria for inviting and removing members from the network. Thus, participants will have to ensure the network is adequately secure.

CONCLUSION

By issuing this Report, FINRA has sought to further the discussion around Blockchain and the regulatory issues associated with its implementation. We are aware of several interesting Blockchain initiatives in other, less-regulated industries, as well as fundraising efforts for such projects using Blockchain tokens. It remains unclear how readily the securities industry will adopt Blockchain solutions.

This client update was originally issued on February 22, 2017.

A Cybersecurity Fine From FINRA

What was broker-dealer Lincoln Financial Securities Corporation expecting when it decided, as so many businesses reasonably do, to turn customer data over to a third-party vendor for hosting in the cloud? Probably not that if the *vendor* got hacked, the Financial Industry Regulatory Authority would bring the hammer down on *Lincoln*. But that is just what FINRA recently did, fining Lincoln $650,000. The case vividly shows how cybersecurity enforcement authorities may seek to hold a firm liable after the fact, even when the firm itself is the victim of a criminal hack.

Back in 2011, a Lincoln supervisory office began to store client records with a cloud vendor. The stored documents included customers' Social Security numbers and other nonpublic personal information. In 2012, a hacker broke into the cloud vendor's systems. FINRA's summary of the case states that the hacker exposed the information of over 5,400 Lincoln customers.

What supported the fine of Lincoln in FINRA's view, and what can the case teach companies in and out of the securities industry?

FINRA's findings:	Potential lessons::
In 2011, FINRA fined two Lincoln entities a total of $600,000 for allegedly failing to secure their web-based electronic portfolio management systems. In connection with the 2016 fine, FINRA concluded that Lincoln—following the 2011 fine—did not adopt "written supervisory procedures," or WSPs,	Enforcement authorities can be particularly tough the second time around. The Federal Trade Commission did not go easy on Wyndham Hotels when it experienced multiple data breaches. Fairly or not, FINRA seems to have taken a tough approach when investigating Lincoln a second time. It bears mention that

FINRA's findings:	Potential lessons::
that were "reasonably designed" to ensure the security of customers' confidential information. Such WSPs are required under FINRA rules and were required at the time under the then-relevant rules of the National Association of Securities Dealers.	the Cybersecurity Framework promulgated by the National Institute of Standards and Technology (NIST), a leading set of cybersecurity standards, suggests that "[r]ecovery planning and processes [be] improved by incorporating lessons learned [from a breach] into future activities."
FINRA concluded that Lincoln's cloud vendor did not use certain cybersecurity measures—specifically, the vendor did not use properly installed antivirus software, nor did the vendor encrypt the stored personal information—and that Lincoln had not ensured the vendor would use these measures.	Enforcement authorities increasingly believe that certain cybersecurity measures are sufficiently well-recognized that not to use them can be deemed unreasonable—*i.e.*, contrary to legal standards. Here, FINRA cited the alleged absence of appropriate antivirus and encryption measures at the cloud vendor. In other cases from the FTC, enforcement agencies and courts, various other shortfalls in cybersecurity have been alleged—such as the lack of multifactor authentication.
FINRA concluded that Lincoln had not sufficiently supported the cybersecurity of its registered representatives. For example, according to FINRA, a Lincoln data security policy required that representatives install firewalls. But, FINRA said, the policy did not describe what type of firewall should be used or how to install it. FINRA	FINRA apparently sees the brand-name, "mother ship" company as having highly specific obligations that extend throughout the network. One might think that a company atop a decentralized network should not be legally obligated to give paint-by-numbers instructions for functions like firewall selection and installation. At least in this case, however, FINRA

FINRA's findings:	Potential lessons::
thus regarded the policy as not meeting the standards for a WSP.	concluded that Lincoln had a duty to be more prescriptive.
FINRA determined that some of Lincoln's registered representatives also engaged vendors to host customer data. But according to FINRA, Lincoln did not monitor or audit the cybersecurity practices of these vendors. FINRA deemed such oversight to be required as part of a FINRA member's "continuing responsibility" under Notice to Members 05-48 to engage in vendor oversight.	At least in FINRA's view, policing the cybersecurity of vendors has gone from best practice to legal obligation. While FINRA was tough on Lincoln here, the issue is not limited to the securities industry. The breaches at Target, Ashley Madison, and the Office of Personnel Management, to name just a few, happened after vendors' credentials were compromised. Options for companies looking to upgrade their vendor oversight might include pre-engagement due diligence, enforcing a rigorous program of access controls, and ongoing testing and verification of vendors' security.
Importantly for Lincoln and its customers, FINRA acknowledged that Lincoln was unaware of any actual misuse of the customer data from the breach in 2012 of the cloud vendor engaged by Lincoln's supervisory office. The additional cloud vendors engaged by registered representatives of Lincoln were not even breached.	At least in FINRA's eyes, neither customer harm nor a breach is necessary to impose cybersecurity sanctions. FINRA cited the purported lack of "reasonable" WSPs, and the purported failure to supervise, as enough in this case to support liability. It is worth noting that FINRA's aggressive posture may not hold in the law generally. For example, a recent federal appeals court decision suggests that more rigorous proof of harm may be required before

FINRA's findings:	Potential lessons::
	the FTC can deem a hacked company's cybersecurity to be an unfair business practice under Section 5 of the FTC Act.
FINRA noted that Lincoln operated through a network of over 500 branches and over 1,100 registered representatives.	Companies operating in a highly decentralized manner are not immune from cyber risk at the far reaches of their business. Many financial services firms use a decentralized model similar to Lincoln's. One can reasonably ask: How fair or practical is it to expect such a company to promote and enforce cybersecurity standards throughout its decentralized network—even to vendors engaged by representatives in distant branch offices? Yet this case indicates that FINRA, at least, seemingly stands ready to impose liability on that basis.

This client update was originally issued on December 5, 2016.

U.S. Data Privacy

"It's free, but they sell your information."

Unsurprisingly, the privacy development that has recently generated the most buzz—the E.U.'s General Data Protection Regulation (GDPR)—originated in Europe, which has long been ahead of the U.S. with respect to privacy regulations. Here in the U.S., data may be used in any way that is not specifically restricted by law and there is no comprehensive privacy law. Instead, there is a patchwork of requirements on both the federal and state levels.

Federally, these laws take a sectoral approach; different laws apply to certain industries, certain conduct, and certain types of information:

- The Gramm-Leach-Bliley Act (GLBA) applies to financial institutions that obtain nonpublic personal information (NPI) from covered individuals, and requires covered companies to safeguard customers' sensitive data and disclose to customers how their information will be handled.
- The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule applies to "covered entity" healthcare organizations and their "business associates." It prohibits disclosure of Protected Health Information (PHI) except with the individual's written authorization, or as otherwise permitted by the Rule. The Rule also requires reasonably designed privacy policies, training of the workforce on privacy policies, and data security safeguards.
- The Video Privacy Protection Act (VPPA) prohibits any "video tape service provider" (an elastic term that dates to the 1980s, but has been applied more recently to video streaming providers) from knowingly disclosing personally identifiable information concerning any customer of the provider except in limited circumstances including to law enforcement, with the customer's written consent, and incident to the provider's ordinary course of business.
- The Children's Online Privacy Protection Act (COPPA) regulates the online collection and use of personal information from children under the age of 13 and prevents websites and online services from collecting, using, or disclosing personal information of children without meeting certain requirements, such as obtaining verifiable parental consent.
- The Telephone Consumer Protection Act (TCPA) governs marketing via telephones and fax machines and automated dialing. Though readers' personal experience might suggest otherwise, the law generally prohibits autodialing or texting wireless phones without consent.

On a state level, California recently—and quickly—passed the California Consumer Privacy Act (CCPA), which takes effect on January 1, 2020, and governs the collection, use, and sale of consumer data by nearly all large and medium sized companies with any presence in California. The CCPA will provide consumers rights regarding their data, and these rights will have significant corresponding obligations for most businesses. The act is likely to reshape U.S. privacy law much as the GDPR reshaped European privacy law, and looks to become the most comprehensive such regime in the United States.

Though U.S. privacy laws are generally less restrictive to companies than Europe's (the CCPA being a notable exception), the patchwork U.S. scheme challenges companies to stay abreast of constant developments and conform their privacy practices to a myriad of laws. This section discusses some of the recent developments and offers practical suggestions for implementing privacy best-practices.

In addition to developments related to the CCPA, TCPA, and VPPA discussed in this section, the Federal Trade Commission (FTC), which has the authority to issue privacy regulations and enforce certain consumer protection laws, has actively investigated and brought actions against companies that the FTC alleges misrepresented their privacy and data protection practices. Uber Technologies, Inc., for example, settled FTC charges that it failed to live up to its claims that it closely monitored employee access to customer and driver data. The original settlement, later revised to account for the revelation that Uber had concealed a data breach, required Uber to implement a comprehensive privacy program and undergo external audits and prohibited further misrepresentation of its privacy practices. VIZIO, a manufacturer of smart TVs, agreed to pay $2.2 million to settle charges that it installed software on its TVs

to collect viewing data on 11 million consumer TVs without consumers' knowledge or consent.

The FTC actions highlight the importance of companies remaining mindful of their privacy and data security obligations in all facets of their business, including in product development, in marketing, and when contracting with third parties. Though guarantees of data privacy and iron-clad data protections may look good on promotional materials, if they do not match a company's actual practices, they may cost the company more in the long-run if they draw FTC scrutiny.

Companies would be wise to evaluate which portions of the U.S. data privacy patchwork cover their operations and take steps to minimize potential liability under those laws. Generally, companies should evaluate what information they collect and why they collect such data. Data should be collected and retained only to the extent and for the amount of time necessary.

Privacy Law Goes Big: California's New Consumer Privacy Act

California has just enacted the biggest and boldest expansion of U.S. privacy law in years: the California Consumer Privacy Act. It was passed by unanimous vote of the legislature on June 28, 2018 and signed the same day by Governor Jerry Brown. The Act moved through the legislative process from start to finish in just a few days. As a result, 18 months from now, California consumers will have broad new rights to access and erase their personal information and to prevent its sale. Covered businesses will have significant new obligations to disclose their privacy practices, limit their use of personal data, and respond to consumers seeking to enforce their new rights. Consumers also will have a new right to sue after certain data breaches.

HOW DID THIS HAPPEN SO FAST?

Credit the heightened privacy awareness that followed Cambridge Analytica. A referendum proposing even tougher privacy standards than the Act's was set to be put before California voters this fall. The legislature thus moved quickly to put its own bill together. The business community basically decided to stand back and let the legislature act—passing a bill that business doesn't love in order to preempt a referendum that it loved even less.

Does the Act Apply to My Organization?

The Act applies to for-profit businesses that meet one of the following three criteria: (1) have $25 million in annual revenue; (2) transact with more than 50,000 California residents' data annually; or (3) derive 50 percent or more of annual revenue from selling the data of California residents. The revenue threshold is

global, not California-specific, and will be increased every two years based on the U.S. Consumer Price Index.

$25 million in revenue and 50,000 consumers are not big numbers in the scheme of things. The legislative intention is clearly to cover virtually all substantial national companies. International, too: there is no exemption for companies based overseas. Note that $25 million in global revenue is all it takes for a for-profit organization to be covered—even if it does not have 50,000 customers in California. Constitutional standards of personal jurisdiction of course would still have to be met for a non-California-based business to be covered.

When Does the Act Take Effect?
January 1, 2020.

What Kind of Data Is Covered by the Act?
"Personal information" is defined very broadly. Any data that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" is covered. Think of it as a "breadcrumbs" definition—whatever might lead back to the consumer is covered. The Act's definition specifically references, for example, Internet activity, geolocation data, employment-related information, consumer purchase histories, biometric data and even "olfactory" information. ("Olfactory" is undefined - one thing among many in the Act that awaits possible clarification by the California legislature or by the state attorney general, who is empowered to "solicit broad public participation to adopt regulations to further the purposes" of the Act.) Going even further, the Act also defines as "personal

information" any "inferences" that could be drawn from any of the listed categories of personal information to create a profile.

What Must Covered Businesses Do Under the Act?
Among other things:

- Disclose to consumers how their personal information is used prior to, or at the time of, collection;
- Inform consumers that they can opt out of the sale of their personal information and that they have a right to have their information deleted;
- Within 45 days of a consumer request:
  - provide details on the consumer's personal information held by the company;
  - disclose what categories of third parties (if any) the customer's personal information has been transferred to;
  - disclose the personal information's source;
  - cease selling, or delete entirely (with some exceptions), the consumer's personal information;
- Provide a clear and conspicuous link on their California-facing homepage titled "Do Not Sell My Personal Information," linking to a location where a user can opt out of the sale of her personal information;
- Provide consumers with at least two methods of contacting the business for information disclosures, including a toll-free number and a website; and
- Train any employee who might receive a consumer's request about his rights under the Act.

Do Businesses Have Any New Rights or Opportunities Under the Act?

For consumers who opt out of the sale of their personal information, the company can impose a charge—but the charge may not exceed the lost revenue from the consumer's choice. A business can also exclude vendors from falling within the definition of third party under the Act by securing contractual commitments from the vendor not to sell the information transferred to them, not to disclose the information outside the business relationship, and to only use the information for the specific purpose for which the personal information is provided to the vendor.

What About Children?

Consumers under 13 continue to be protected primarily by the federal Children's Online Privacy Protection Act. The Act adds new protections as well. Sale of consumer data for consumers under 13 can only take place on an "opt-in" basis, *i.e.*, if the child's parent or guardian has affirmatively consented. The same is true for consumers between 13 and 16, except that those consumers can give their own consent.

What About Data Breaches?

California consumers whose data is exposed in a breach now can recover statutory damages ranging from $100 to $750 per California consumer per incident. The Act does contain safe harbors for companies that experience a breach, including a 30-day cure period (likely only applicable to small personal information incidents). There is a requirement that, prior to filing suit, plaintiffs notify the California Attorney General, who has a right to bar the consumer plaintiffs from bringing suit. There is no attorneys' fees provision.

Notably, the Act's broad new definition of "personal information" is not exported to the data breach arena. The new private right of action kicks in only when the pre-existing breach notification law's narrower, more traditional definition of personal information is met. That definition covers a person's "first name or first initial and his or her last name in combination with" data elements such as a financial account number (plus any required password), SSN, driver's license number, or username or email address (plus password). In short, disclosure of "breadcrumbs" is not defined as a breach and triggers no right to sue.

Who Can Enforce the Act?

The California Attorney General may bring civil actions to fine companies that are found noncompliant. There is no consumer private right of action other than for data breaches. The Act says that nothing in it "shall be interpreted to serve as the basis for a private right of action under any other law." This appears to mean no suits for violations of the Act will be permitted under California's general consumer protection statute, Section 17200 of the Business and Professions Code. Unlike the comparable laws of most other states, Section 17200 allows suits for acts that are not just "unfair" or "deceptive" but "unlawful." This can allow for Section 17200 to serve as a back door to a private right of action under other laws that do not themselves allow one. The legislature appears to have closed that back door here.

How Does the Act Compare to the GDPR?

The Act is similar, but not identical, to the GDPR:

THE ACT	THE GDPR
Covers only for-profit entities meeting one of three threshold criteria, based on revenue or volume of information collected. Doing business with 50,000 or more Californians is one of the three possible grounds for coverage, but is not required.	Covers processing of personal data by all entities (for-profit or nonprofit) with an "establishment" in the EU, or entities outside the EU who offer goods and services to individuals in the EU (a/k/a monitoring or targeting EU data subjects from outside the EU).
Defines "personal information" broadly to include broad categories of data that directly or indirectly identifies a person. Publicly available information is excluded.	Defines "personal data" broadly to include broad categories of data that directly or indirectly identifies a person. Publicly available information is included.
Requires third-party vendor agreements to prohibit vendors from retaining, using or disclosing personal information for any purpose besides the services to be performed.	Requires third-party vendor agreements to contain a standard set of commitments to compliance with GDPR standards.
Grants consumers the right to be informed of, to access and (in more limited circumstances) to obtain deletion of their personal information.	Grants consumers the right to be informed of, to access, to correct, (in more limited circumstances) to delete, to restrict processing of and to obtain a portable copy of their personal data.
Grants consumers the right to opt out of the sale of their personal information.	Requires entities to have a lawful basis for processing information if not seeking consumer consent.

Is the Act Likely to Change Before It Goes into Effect in 2020?
Lobbying efforts to make the Act more business-friendly will surely continue. The California legislature has the right to amend the Act. It would not have had the right to amend a law passed by referendum. This appears to be why the business community elected not to fight the bill's rush to passage.

Is the Act Effectively a New National Standard?
Not directly. On its face, the Act only applies directly to how your organization treats California consumers. Very possibly, the Act may set a new standard in a practical sense. First, other states have been known to follow California's lead on privacy law. Nobody should be surprised if other state legislatures now pass similar bills. Second, companies will face a tough choice. They can voluntarily apply the burdensome terms of the Act to all their consumers regardless of state of residence or create a whole set of policies, procedures and platforms just for handling the personal information of Californians. The all-consumers approach may prove operationally easier for many companies.

What Should Businesses Do to Prepare?
Businesses across the country and the globe should start by determining if they fall within the scope of the Act at all. For the many that do, the good news is you have 18 months to get ready:

- Evaluate the pros and cons of complying just as to California consumers vs. complying as to all consumers. Pick an approach.
- Consider the technical measures and company policies that will be necessary. Start drafting.
- Then implement and test your procedures for responding to consumer requests and meeting corporate obligations. Companies

may want to run simulation drills a la tabletop exercises in cybersecurity.
- Robust data mapping will help ensure effective response to data access and deletion requests. You can't provide it or purge it if you don't know where it is.
- Consider whether there are lobbying efforts, perhaps being conducted by trade associations in your industry, that you would like to join in order to seek legislative reform of the Act—or the issuance of clarifying regulations—before the Act takes effect.

This client update was originally issued on July 3, 2018.

D.C. Circuit Court Decision May Help Level the Playing Field for TCPA Defendants

In recent years, the Telephone Consumer Protection Act ("TCPA") has imposed significant burdens on companies in the financial services, collections, and retail industries that use automated dialing equipment (commonly known as "autodialers") to reach large volumes of consumers or account holders. The TCPA, a 1991 statute, prohibits using an Automated Telephone Dialing System ("ATDS") to call or send text messages to a cellular telephone number without prior express consent. Before 2010, there were at most a few hundred TCPA suits filed each year. Since 2011, that number has mushroomed to thousands of lawsuits filed annually.

Defending against the TCPA is particularly challenging because the TCPA is a strict liability statute: If a company has autodialed someone who has not provided prior express consent, there are few, if any, available defenses. Moreover, each autodialed call or text message sent to a cellular telephone number can result in a fine of up to $1,500. There are many instances in which courts have been willing to certify TCPA class actions consisting of thousands or more of call recipients who were allegedly called without prior express consent. Companies who are defendants in such cases may face potential litigation exposure of hundreds of millions—or even billions—of dollars. As a result, TCPA settlements in excess of $10 million are not uncommon, and there have been TCPA settlements as high as $76 million. In one TCPA case that went to trial, the defendant—an entity that autodialed a list of telephone numbers that it had purchased—faced a $1.2 billion verdict (although the judge subsequently reduced it to $32 million).

In 2015, the Federal Communications Commission ("FCC"), which is responsible for implementing the TCPA, exacerbated the proliferation of TCPA litigation by issuing a Declaratory Ruling and Order (the "2015 Order") which was very friendly to the plaintiffs' bar. Among other things, this Order included a very expansive definition of what qualifies as an ATDS and provided almost no protection from liability for companies who were attempting to reach consenting consumers whose numbers had, unbeknownst to the companies, subsequently been reassigned to third parties.

The FCC's order had a dramatic effect on TCPA litigation. According to a 2017 study by the U.S. Chamber of Commerce, in the 17 months before the 2015 Order was issued, there were 2,127 TCPA lawsuits filed; after the Order was issued, there were 3,121 lawsuits filed during the same period of time—an increase of nearly 50 percent.

However, a recent decision by the Court of Appeals for the D.C. Circuit in *ACA International v. FCC* (No. 15-1211) may provide much-needed relief for defendants. The decision invalidated the most plaintiff-friendly portions of the 2015 Order and is likely to make it more challenging for plaintiffs to bring TCPA cases, particularly against companies that make concerted efforts to autodial only consenting consumers. Furthermore, the decision gives the FCC an opportunity to clarify its rulemaking at a time when the Commission's leadership is much more favorably disposed to business interests.

The court's decision has potential impact concerning four key issues:

THE DEFINITION OF "AUTOMATED TELEPHONE DIALING SYSTEM"

One inherent problem with the TCPA lies in the difficulty of categorizing modern dialing equipment according to a statutory definition that is more than 25 years old. The TCPA applies only to calls made to cellular telephones using an ATDS, which is defined as "equipment which has the capacity—(a) to store or produce telephone numbers to be called, using a random or sequential number generator; and (b) to dial such numbers." This definition was originally written to apply to autodialers that dialed randomly generated numbers. Today, however, many companies use far more sophisticated predictive dialers that dial lists of numbers assembled by a company, typically from its consumer records. Predictive dialers use strategies that are designed to make calls at times when agents are anticipated to be available.

In its 2015 Order, the FCC chose to interpret the definition of ATDS broadly, stating that a dialing device falls within the definition of an ATDS merely if it has the "potential functionalit[y]" to carry out the tasks specified by statute, regardless of whether the functionalities are actually installed on the device or the functionalities are actually used during the call at issue. The D.C. Circuit struck down this definition for two reasons:

First, defining "capacity" in terms of "potential functionalit[y]" was unreasonable because it was so broad that it would include personal smart phones, given that there are apps which can dial random or sequentially generated telephone numbers. The court concluded that Congress never intended the TCPA to apply to calls placed by widely used devices.

Second, the court criticized the FCC for being "of two minds" when interpreting the key statutory phrase, "using a random or sequential number generator." In some places, the court explained, the FCC's prior statements have suggested that it believes that an ATDS must be able to generate random or sequential numbers and then dial those numbers. Yet in other places, the FCC has stated that dialing equipment such as predictive dialers count as ATDS even though predictive dialers do not generate random or sequential telephone numbers. The court found that the 2015 Order's "lack of clarity about which functions qualify" a device as an ATDS was a further reason to invalidate the FCC's ATDS definition.

Potential Impact

It is too early to assess the significance of this portion of the court's decision because the FCC has not issued a new definition of what counts as an ATDS. There are at least three approaches the FCC could take:

- The FCC could issue a broad ATDS definition that encompasses automated calls to lists of telephone numbers assembled by a company but that excludes smartphones. Since businesses typically do not use smartphones to contact consumers, such a decision would essentially maintain the status quo.
- The FCC could issue a very narrow ATDS definition that consists only of a device that currently has the capacity both to (i) generate random or sequential numbers and (ii) autodial such numbers. Such a ruling could exclude from the TCPA's scope predictive dialers or similar equipment that are configured only to call pre-existing consumer lists. This definition would likely curtail TCPA litigation.

- The FCC could adopt a middle-ground approach. In 2015, FCC Commissioner Ajit Pai—who is now Chairman of the FCC—objected to the 2015 Order in part on the grounds that the TCPA was never meant to interfere in communications between businesses and their customers. Based on that logic, the FCC could take the position that the ATDS definition does not include calls made by businesses to their customers but does include calls made from businesses to lists of individuals that were purchased from third parties.

CONSEQUENCES OF CELLULAR TELEPHONE NUMBER REASSIGNMENT

Each year, millions of cellular telephone numbers are reassigned. This can happen for a number of reasons, including because consumers change cellular telephone service providers or because consumers use pre-paid cellular telephones for a short period of time. Both of these phenomena occur frequently among low-income individuals—a population that frequently receives automated calls from collections agencies and credit card companies. If a company calls what it believes to be the cellular telephone number of a consenting consumer, but the consumer's telephone number has been reassigned since the consent was provided, the company is likely to reach an unknown individual who has not consented to being autodialed by the company. Because the TCPA is a strict liability statute, the caller may be liable in that circumstance. "Wrong number" TCPA class actions thus have become an increasingly common claim against businesses that engage in direct contact with consumers or account holders.

Because the TCPA holds callers strictly liable, the very first call to a cellular telephone number following reassignment arguably violates

the TCPA. In its 2015 Order, the FCC recognized that this interpretation was overly "severe." In response, the FCC clarified that the TCPA allowed for "reasonable reliance" on the prior express consent provided by the telephone number's original holder. The FCC created a "safe harbor" that allowed one call to a telephone number after reassignment without incurring a TCPA violation. Any subsequent telephone calls, however, would violate the statute—regardless of the outcome of the first call. In other words, if the first call went unanswered, the caller would be liable for all subsequent calls, even though the caller might still be unaware that the number was reassigned.

In its decision, the court upheld the application of "reasonable reliance" in this scenario, but invalidated as arbitrary the FCC's limitation of the "safe harbor" provision to just one call. The court criticized the FCC for assuming that a caller could engage in "reasonable reliance" for only one call after reassignment, as even the FCC acknowledged that the first call might not provide any indication that the number had been reassigned. As a result, it might well be reasonable to rely on the previously-obtained consent for more than one call.

Potential Impact

This ruling is a significant victory for companies that autodial consumers because it bolsters their defenses against "wrong number" TCPA cases in two substantial ways.

First, the decision may facilitate companies' ability to prevail on the merits of individual TCPA claims if they can argue that the court's decision strongly suggests that multiple calls to a reassigned number should not result in a violation if the company acted reasonably. A

defendant would likely be in a strong position to argue that it acted reasonably if it could establish, for example, both that (i) it had recently verified that the telephone number at issue belonged to the consumer (either because of recent contact with the consumer or because a vendor confirmed that the consumer's name was likely associated with the telephone number) and (ii) the company stopped calling the telephone number after it was first informed that the telephone number was reassigned.

Second, the decision is likely to be even more significant for defeating class certification. Doing so is essential for TCPA defendants because if a large class is certified, a defendant faces a potentially enormous verdict based on statutory per-violation damages. A class cannot be certified, however, where resolution of the class members' claims would require individual inquiries. While the plaintiffs' bar argued that evaluation of the uniform "one call" safe harbor rule can be managed on a class-wide basis, the D.C. Circuit's decision suggests that "reasonable reliance" will become more tailored to the specific facts of interactions with individual call recipients. Such "reasonableness" inquiries cannot be conducted on a class-wide basis.

Despite this potential implication, however, companies should not think that they now have license to relax controls to ensure TCPA compliance. The argument that individualized inquiries are required for each alleged "wrong number" call is likely to be strongest when the company can convince the court that it has procedures in place to ensure that it is calling only numbers of individuals who have provided prior express consent and that "wrong number" calls are the exception, not the norm. To that end, companies that autodial consumers should maintain for at least four years—the TCPA's

statute of limitations—evidence both of consumer consent and of the disposition of its calls with consumers. Companies should also avoid calling lists obtained from unrelated third parties, as it is likely to be difficult to argue that those call recipients provided prior express consent.

REVOCATION OF CONSENT

The 2015 Order provided that a called party may revoke consent to receiving autodialed calls "through any reasonable means," whether orally or in writing. Although the court agreed with this position as a default rule, it specifically noted that the 2015 Order does not preclude a company from entering into a contract with the called party which specifies the means by which consent may be revoked.

Potential Impact

This portion of the court's decision highlights that companies may be able to include clauses in agreements with their consumers which provide that consent can only be revoked in writing. This is an option that companies may wish to explore. If a company requires revocation of consent in writing, it may be easier for the company to later defend itself against a TCPA lawsuit. A case will quickly collapse if the plaintiff cannot substantiate that she followed the procedures to which she agreed for revocation of consent.

EXEMPTION FOR CERTAIN HEALTHCARE-RELATED CALLS

The 2015 Order provided that calls with a healthcare treatment purpose—including appointment and exam confirmations and reminders, wellness checkups, lab results, home healthcare instructions and information related to hospitalizations—are exempt from the requirement to obtain prior express consent. The court rejected the argument that the exemption should also have covered

communications relating to accounting, billing and debt collection. The court explained that communications about financial issues, as opposed to issues relating to treatment, did not warrant an exemption from the TCPA.

Potential impact

This portion of the opinion simply codifies the status quo. However, the FCC provisions governing when the "healthcare exemption" applies are quite detailed and companies that rely on these provisions should ensure that they are complying with all of the applicable requirements. Healthcare companies should, wherever practical, seek prior express consent from all consumers and thus eliminate need to rely on this TCPA exemption.

* * *

In the aftermath of the court's decision, the FCC now has the opportunity to engage in new TCPA rulemaking. Since the 2015 Order was issued, there has been a significant change in the FCC's leadership, which is concerned about the proliferation of TCPA litigation. The court's decision gives that leadership the opportunity to issue new rules that will curtail litigation against companies that are making good-faith efforts to call only consumers or account-holders who have consented to being autodialed. Affected businesses should carefully monitor the FCC's rulemaking and where appropriate, consider offering comments on proposed new rules.

This client update was originally issued on March 29, 2018.

New Decision Confirms Narrow Meaning of "Personally Identifiable Information" Under Video Privacy Statute

The Ninth Circuit recently dealt another blow to attempts to expand corporate liability under the Video Privacy Protection Act ("VPPA"). In *Eichenberger v. ESPN*, the Ninth Circuit affirmed the district court's dismissal of a VPPA class action that accused ESPN of disclosing personal information in the form of a device serial number. The Ninth Circuit held that disclosures of personally identifiable information ("PII") are only actionable if they "readily permit an ordinary person to identify" a specific individual, which device numbers don't do.

VPPA prohibits a "video tape service provider" from disclosing "information which identifies a person as having requested or obtained specific video materials or services."[1] VPPA was enacted in 1987, after the clerk at a neighborhood video store handed a reporter the tape rental history of Judge Robert Bork. Congress provided for liquidated damages of $2,500 per violation, plus attorneys' fees—amounts that would yield eye-popping damages at Internet scale. The plaintiffs' bar thus has filed class actions against a host of online video companies.

These cases all rest on a simple premise: The company providing an online video to you typically also provides information about the viewing session to third parties, like advertising service companies and analytics firms. This information usually takes the form of an anonymous number string, such as the device identifier on your smartphone. Plaintiffs argue that sharing these anonymous number

[1] 18 U.S.C. § 2710(a)(3).

strings is the digital equivalent of the video store clerk handing over a hard copy of Judge Bork's tape rental history.

Whether plaintiffs are right depends on whether the number string associated with your viewing session "identifies a person" within the meaning of VPPA. Put another way: When Video Streaming Company tells Analytics Firm that it has just sent video XYZ to device number 123456, does that "identify" John Smith as the owner of the device? Plaintiffs have argued that it does, because there are various ways of connecting the dots between device identifier 123456 and John Smith.

At issue in *Eichenberger* was the device identifier of a Roku box. The Ninth Circuit said that the identifier alone wasn't enough under VPPA: a Roku device identifier "cannot identify an individual unless it is combined with other data." Indeed, the Ninth Circuit emphasized that only a "complex" process "to link an individual's Roku device number with other identifying information derived from an enormous amount of information collected from a variety of sources" would allow a third party to identify an individual. That meant that the Roku identifier alone wasn't PII.

The Ninth Circuit joined the Third Circuit, in *In re Nickelodeon Consumer Privacy Litigation*, which held that PII "means the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."

Both *Eichenberger* and *Nickelodeon* distinguished a First Circuit case, *Yershov v. Gannett Satellite Info. Network, Inc.* There, the First Circuit held that an iPhone device ID, when disclosed along with GPS

coordinates, was PII under VPPA. For now, the still-emerging law in this area seems clear: anonymous number strings are not PII "without more," and *Yershov* is an outlier that went plaintiffs' way because of the identifying power of GPS data.

Eichenberger was not a complete success for the defense: The Ninth Circuit joined others in holding that VPPA plaintiffs have standing even though the disclosures did not cause them real-world harm. Courts have reasoned that VPPA codifies a substantive right to privacy, and that this is constitutionally sufficient to create a case or controversy under Article III granting plaintiffs standing. The Supreme Court's 2016 *Spokeo* decision, which created a test for standing in statutory privacy cases, has been of little help to VPPA defendants thus far.

This area of the law is evolving rapidly. Some best practices include:

- **Know that you're a potential VPPA defendant. Compliance starts with awareness of risk**. Companies whose core business involves video streaming (like Netflix, Hulu, ESPN, CNN and Viacom) have all been hit with VPPA suits. But in a world where virtually all companies provide some form of streaming video on their websites, everyone's a target.
- **Know what information you're passing to which third parties**. This isn't always easy to tell; the ecosystem of online video delivery is complex and involves a host of players. Consider how the flow of information to third parties can be kept to a minimum. Then revisit your processes regularly: the flow of information may be different a month or a year from now.

- **Watch this space**. VPPA litigation remains ongoing. The narrow definition of PII adopted in *Eichenberger* and *Nickelodeon*, while clearly correct, could evolve. Even today, that definition does not necessarily apply in other contexts. The FTC staff, for example, takes the view that "data that is reasonably linkable to a consumer or a consumer's device is personally identifiable." The staff thus cautions that companies should avoid making broad statements in their privacy policies that they are not collecting PII. Likewise, EU law may treat IP addresses and other anonymous digital data as PII in contexts where U.S. law would take a different approach.

This client update was originally issued on December 11, 2017.

Badger Breach: Good Housekeeping?

The data breach just disclosed by the University of Wisconsin isn't the biggest you'll ever hear about. Only 1,213 individuals had their names and Social Security numbers exposed to a digital intruder. But it might be the best reminder in a while of a crucial cybersecurity maxim: Nobody can breach what you don't have.

WHAT HAPPENED?

Last month, an intruder gained access to a database that held information belonging to former applicants to the University of Wisconsin Law School. The breached information consisted of paired names and SSNs from 1,213 individuals who had applied in 2005-06.

Since discovery of the breach, the proverbial "series of unfortunate events" has unfolded, just as in a bigger breach. As required by state law, the university sent notice to the affected individuals—in this case, by both postal and electronic mail. The university notified law enforcement, which continues to pursue the hacker. The university reviewed its cybersecurity and announced improvements. It offered the individuals a year of free credit monitoring at the university's expense. And a slew of news stories publicized the breach, inflicting reputational harm on a great institution.

WHAT CAN BE LEARNED?

Though cybersecurity often presents complicated technical questions—Are we encrypting the data? Is file integrity being monitored?—the Badger Breach shows that simpler questions matter too:

- Do we need to collect that personal data in the first place? In its FAQ on the breach, Wisconsin stated that it must collect SSNs to match admission applications to applications for financial aid. Other organizations might take the episode as a prompt to ask: what forms are we using, what personal data do those forms request, and what business purposes if any do each of those data points really serve? A self-assessment along these lines can be as useful as an encryption upgrade in reducing an organization's attack surface.
- If we need to collect that personal data, how long do we need to keep it? Wisconsin's FAQ does not state why applicant data from 2005-06 were still being held. The incident can be taken as a prompt to ask whether your organization might be holding on to stale data. Consider a thorough exercise in data mapping—that is, a systematic survey of what you are holding onto, why, and where. The exercise may turn up old datasets that would only be interesting to a hacker.

We know of one large employer that conducted a systematic review of all instances where it was collecting SSNs across the organization. The employer determined that, in numerous instances, it actually had no compelling need to collect the SSNs. By ceasing to collect the data and purging what it had, the organization significantly reduced its exposure to a breach.

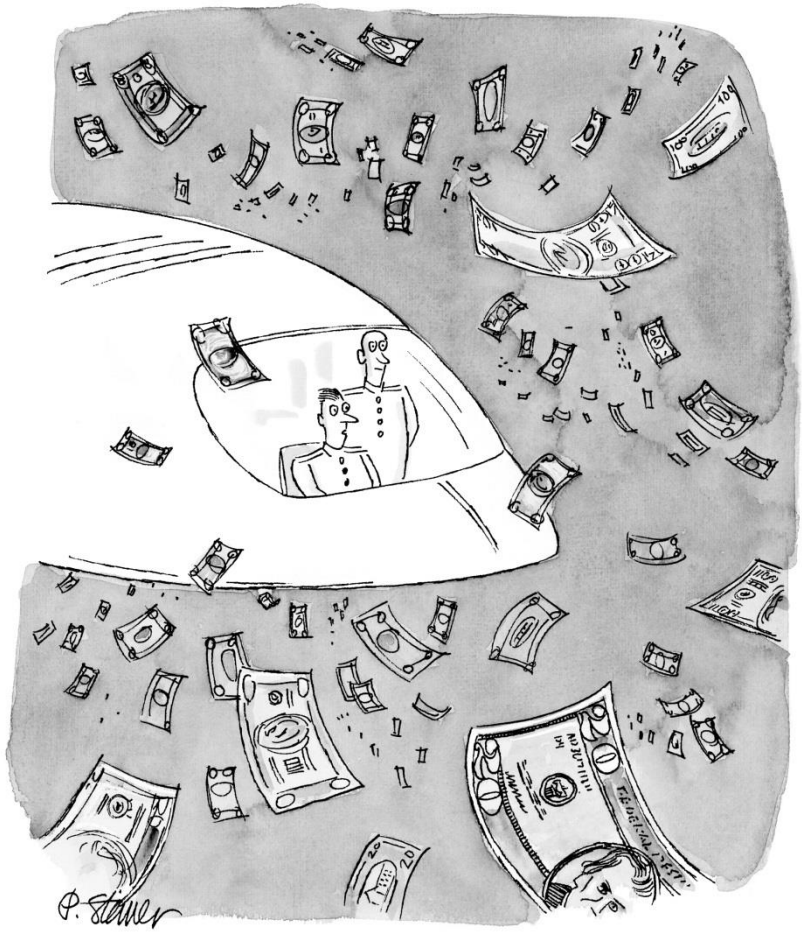
Good cyber housekeeping supports legal compliance and vice versa. U.S. and European authorities alike have underscored that "data minimization" is necessary to protect both data security and data privacy. In one enforcement case, the U.S. Federal Trade Commission ticked off a list of reasons why it believed a company's cybersecurity was so poor as to be unlawful. Besides a number of technical failings, the FTC noted, the company "never deleted any of

the consumer data it had collected." (The case is now on appeal, on grounds largely unrelated to this conclusion.)

The technical side of cybersecurity is critical and cannot be minimized. But the Badger Breach highlights how important it also is to review those boring old document retention policies; to enforce them; and to periodically review what data you are collecting and why. Simply put: If you never collect it, or securely discard it, then no hacker could ever endanger it. On, Wisconsin!

This client update was originally issued on December 12, 2016.

Global Survey



"Captain, it looks like we've entered cyberspace."

While the European Union's General Data Protection Regulation ("GDPR") has dominated the news this past year, regulators around the world are increasingly paying attention to company data privacy and cybersecurity practices. Some regulations are sector-specific, aimed at critical infrastructure providers, while other guidance hones in on certain topics, such as personal data localization. All reflect the importance of maintaining good data privacy and cybersecurity hygiene in today's regulatory landscape.

Russia, for example, has passed broad, strict regulations on how personal data of Russian citizens can be collected, where it can be kept, and how it can be transferred. The failure to process personal data with the necessary consent or for the appropriate objectives, or even the failure to publish a personal data processing policy, can lead to administrative fines from the Federal Service for Oversight in the Sphere of Communications ("Roskomnadzor"). Violating localization obligations by accumulating or storing personal data of Russian citizens in databases located outside of Russia could lead to an even heavier penalty, the restriction of a company's access to Internet resources. Roskomnadzor now also supervises companies that facilitate exchange of electronic messages via the Internet without a telecom carrier ("messengers") and providers of digital videos and video streaming via over-the-top platforms ("online cinemas"). The gradual, but consistent, expansion of Roskomnadzor's oversight indicates that companies should keep up-to-date with Russian regulations.

Localization obligations form part of the Chinese regulatory landscape as well. China's Network Security Law, which went into effect last summer, requires "Critical Information Infrastructure" operators to store in China data that is collected or generated in China. The Network Security Law also catches "Network Operators,"

a sweeping term that includes any provider of online information and services. Not only must Network Operators obtain consent before collecting and using personal data, they must also monitor information published by users. Local authorities promptly began taking enforcement action against social media platforms, technology companies, and e-commerce platforms—though many of the penalties have been relatively light.

Nearby in Hong Kong, brokers face increasing scrutiny of their privacy and cybersecurity practices. This summer, for example, all persons licensed by or registered with the Hong Kong Securities and Futures Commission and engaged in internet trading must implement 20 baseline cybersecurity requirements, including two-factor authentication, encryption, and mandatory client notification of certain user account events. In May, the Securities and Futures Commission also issued a circular about security measures and record keeping practices for companies that receive client orders through instant messaging. Keeping an eye out for these circulars will help companies stay abreast of best practices for the securities industry and stay ahead of the regulatory curve.

Back in Europe, national data protection authorities ("DPAs") are scrutinizing cybersecurity and data privacy practices more intensely, in line with the GDPR regime. The United Kingdom Information Commissioner's Office's recent response to the Carphone Warehouse breach, for example, reflects greater focus on the technical safeguards a company has in place at the time of a breach. Autoriteit Persoonsgegevens, the Dutch DPA, has indicated a greater willingness to impose fines. The Irish DPA will take a closer look at privacy policies. Companies that have not yet implemented a GDPR compliance plan should prioritize bringing their data security practices up to speed quickly.

Elsewhere, regulators have expanded on existing data privacy and cybersecurity obligations. Data breach notification is now mandatory in Australia and Canada. In Latin America, the Ibero-American Data Protection Network released a set of Standards for Data Protection in 2017. These Standards were developed in reference to the GDPR, featuring a similar emphasis on transparency and proportionality, as well as restrictions on processing and rights for individuals.

As the articles in this section illustrate, there is an unmistakable, global convergence of legal obligations, industry standards, and regulatory expectations. Going forward, data privacy and cybersecurity will need to be top of mind for any company conducting international business.

Carphone Warehouse Breach

UK TELECOMS RETAILER FINED £400,000 FOR DATA SECURITY FAILURES – WHAT CAN OTHERS LEARN?

On 8 January 2018, the Information Commissioner's Office (ICO) fined leading telecoms retailer Carphone Warehouse £400,000 for having inadequate technical and organisational measures to safeguard employee and customer personal data. The ICO's Penalty Notice provides useful guidance to companies on technical and organisational safeguards they may be expected to have in place to secure personal data. With higher potential penalties for such failures under the forthcoming EU General Data Protection Regulation ("GDPR"), businesses handling personal data should consider whether their safeguards and controls suffer from any of the deficiencies for which the ICO fined Carphone Warehouse.

Why did the ICO fine Carphone Warehouse?

Between 21 July and 5 August 2015, attackers apparently targeted a collection of Carphone Warehouse's virtual servers which hosted internal and external websites. The ICO Penalty Notice reveals that the system housed a large volume of personal data: over 3.3 million customer records, historic payment details for over 18,000 payment cards and approximately 1,000 employee records.

According to the ICO, the attackers scanned the system with a penetration testing tool to identify vulnerabilities. The attackers then seemingly gained access to the system either by using vulnerabilities in an outdated content management system or valid administrator credentials from an unknown source. Having gained access to the system, the attackers had—at a minimum—access to a large volume of personal data, with indications that some of it may have been exfiltrated. Carphone Warehouse apparently became

aware of the breach and began to take remedial steps on 5 August 2015 when unauthorized decryption activity was detected and raised the alarm.

Having investigated the incident after Carphone Warehouse self-reported, the ICO determined that the company's safeguards had "multiple, systemic and serious inadequacies" which merited the £400,000 monetary penalty.

What could Carphone Warehouse have done better?
In its Penalty Notice, the ICO identified organisational and technical failings that it considered to constitute breaches of Carphone Warehouse's data protection obligations. Notably, the ICO reached this view irrespective of whether the specific failings contributed to the data breach. Those failings, along with key takeaways for companies, are noted below.

- *Out-of-date software*. The ICO identified that key elements of the system's software were significantly out of date. Despite having a "Patch Management Standard" in place, Carphone Warehouse did not follow it. This lapse resulted in what the ICO felt were serious, and avoidable, vulnerabilities. Likewise, contrary to the company's policy, anti-virus software was not installed on the relevant servers. While paper compliance in the form of written procedures and manuals is important, companies should consider conducting periodic reviews of their processes to ensure that their written policies are followed in practice. If there are good reasons for deviating from those policies, then deviations should be formally approved and their rationale recorded.
- *Inadequate credential management*. The ICO found that Carphone Warehouse failed to adequately manage login credentials. The company had no credential misuse detection system and the root

password for several server operating systems was the same and known to 30-40 employees. Companies should limit access (and, in particular, administrator-level access) to systems containing personal data and have measures in place to detect misuse of valid credentials. This can help increase the prospects of early incident detection and mitigate damage.

- *No Web Application Firewall* ("WAF"). It appears from the Penalty Notice that when the attack occurred, Carphone Warehouse did not have a WAF to monitor and filter traffic to and from its web applications. While it was unclear whether a WAF would have prevented the attack, the ICO identified this as a significant failing and its absence contrary to accepted industry security practice. Beyond the benefits of a WAF, the ICO's comments suggest that companies should routinely revisit their security infrastructure to ensure that it meets industry standards as technologies advance and best practices evolve.
- *Insufficient vulnerability and penetration testing*. The ICO discovered that Carphone Warehouse had not performed routine testing procedures, such as internal or external penetration testing, in the 12 months preceding the attack. This indicates that the ICO, like many other regulators, views annual penetration testing as a practice that may be required to comply with the obligation to implement adequate measures to safeguard personal data. Notably, Carphone Warehouse's policy called for annual testing but the policy was not followed.
- *Over-inclusive and unsecure data retention*. The ICO found that the compromised systems held old transaction data including credit card details for no good reason; in fact, Carphone Warehouse apparently acknowledged that it did not know the data had been retained on the system. Moreover, although the data were encrypted, the decryption keys were stored in plain text in the application's source code, and were therefore easily accessible to

hackers. Data minimisation—that is, storing personal data for no longer than is necessary—is a key data protection requirement, and companies need to implement processes to keep track of what data they hold and purge it when it is no longer needed. Where personal data are retained, they have to be stored securely, and encryption should meet prevailing industry standards and be updated as they evolve.

THE FUTURE UNDER THE GDPR

While the fine may be the same size as the one that the ICO gave TalkTalk in 2016, the ICO's Penalty Notice is notable for the greater depth in which it addresses Carphone Warehouse's technical failures; perhaps signaling that the ICO will, in the future, subject companies' technical safeguards to greater scrutiny. Lessons that other companies learn from Carphone Warehouse's experience will also become increasingly important in May 2018, when the GDPR comes into force. Not only does the GDPR significantly increase fines for non-compliance, but it also engages with technical security requirements in much greater detail than the current Data Protection Directive. It is therefore likely that, as time goes on, EU Data Protection Authorities will increase their focus on technical safeguards, as the ICO had done in this case. Companies should consider getting ahead of this trend by taking steps to improve their data security procedures and controls and ensure that those procedures and controls are followed in practice.

Debevoise advises businesses, both in and outside of the European Union, on all aspects of GDPR and cybersecurity preparedness and breach response.

This client update was originally issued on 18 January 2018

Seven Takeaways from the UK Government's Cybersecurity Regulation and Incentives Review

Building on the UK Government's recently issued cybersecurity strategy,[1] the UK Department for Culture, Media & Sport has published its Cyber Security Regulation and Incentives Review (the "Review").[2]

After considering the need for regulation or incentives to boost cyber risk management in the UK, the Review rejected calls for prescriptive cybersecurity regulation. It instead concluded that, at least for now, cybersecurity regulation is unnecessary beyond the forthcoming EU General Data Protection Regulation ("GDPR") and sector-specific regulation such as that arising from the EU Network and Information Systems Directive.

While non-binding, the Review also highlighted measures that organisations may wish to implement to improve their cybersecurity posture. Businesses may, therefore, consult the Review for guidance on how to bolster their cyber-defences.

THE TAKEAWAYS

First, GDPR-preparedness is inextricably linked to cybersecurity. The Review affirmed that meeting the GDPR's enhanced data protection

---

1 *See* "UK Government Launches Five Year National Cyber Security Strategy" (November 2016), http://www.debevoise.com/~/media/files/insights/publications/2016/11/20161102_uk_government_launches_five_year_national_cyber_security_strategy.pdf.

2 *See* Department for Culture, Media & Sport, "Cyber Security Regulation and Incentives Review" (December 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf.

requirements will be integral to robust cybersecurity. This echoes the Government's five-year cybersecurity strategy which identified the GDPR, which comes into force in May 2018, as a key lever for improving cybersecurity in the UK. Businesses should, therefore, consider integrating GDPR-preparedness with their cybersecurity programme. This may include ensuring that their cybersecurity incident response plan recognises the GDPR's mandatory breach notification requirements.

Second, businesses should pursue pro-active and dynamic cyber risk management. The Review warns that a tick-box compliance culture can become outdated quickly in the fast-moving world of cyber threats. It, therefore, encourages organisations to develop a pro-active approach to cyber risk management. This includes having procedures and tools to monitor and pre-empt cyber threats, as well as implementing an effective incident response plan to resolve issues swiftly when they arise. A key part of this is establishing an organisational structure with clear allocation of roles and responsibilities among internal individuals and teams and external advisers.

Third, businesses with reporting obligations should consider whether their reports should address cybersecurity risk. While the Government is not pursuing mandatory cybersecurity annual reporting, the Review notes that around two-thirds of FTSE companies include information on cybersecurity risks in their annual reports. Investors are also increasingly interested in cybersecurity and organisations should, therefore, be mindful of their reporting obligations.

Fourth, cybersecurity "health checks" can be a valuable cyber risk management tool. While the Review found against implementing mandatory cyber health checks, the Government recognises their benefits. Businesses should, therefore, consider whether a cybersecurity audit of their technical, legal and organisational structures might prove useful when reviewing their cybersecurity systems and controls.

Fifth, there is a strong business case for robust cybersecurity. The Review stresses that it is in organisations' own commercial interests to invest in cybersecurity and ensure that they have appropriate systems and controls in place to deter and deal with breaches. Even businesses which hold limited personal data may be targeted for their IP, trade secrets or other sensitive information. Accordingly, businesses with relatively limited exposure to the increased obligations and penalties under the GDPR should still recognise the importance of mitigating their cybersecurity risk profile.

Sixth, the Government is not mandating specific cybersecurity controls, risk management practices or systems. It understands that each organisation has unique IT systems and hence different technical requirements. Businesses will, therefore, have the latitude to explore and design their cybersecurity posture in a way that best suits their specific cyber risks and business needs. Nevertheless, businesses may find it useful to keep abreast of the National Cyber Security Centre ("NCSC") and Information Commissioner's Office

guidance to adhere to emerging best practices, and learning from recent enforcement actions which indicate regulators' expectations.[3]

Seventh, cybersecurity is a shared responsibility. The Review makes clear that, contrary to the trend in other areas of regulatory enforcement, individuals will not be targeted for enforcement action in cases of cyber breaches. Instead, the Government will focus on organisations as a whole, not pinning responsibility on a single individual, with the hope of encouraging a culture of pro-active responsibility-taking (especially on boards), rather than penalisation. The NCSC will also work with a range of partners to ensure investors and shareholders have the tools to build effective partnerships with company boards to influence behavioural change.

CONCLUSION

The Government remains committed to developing an environment that incentivises improved cybersecurity without unnecessary business burdens. While the Government has decided not to implement prescriptive cybersecurity regulations, businesses should not forget the demands of pre-existing and future data protection obligations, most notably the GDPR, on their cybersecurity programmes. Those operating in the financial services sector should also heed the Financial Conduct Authority's recent statements that it expects all regulated firms to have a pervasive security culture.

Organisations should also recognise the business case for robust cybersecurity beyond simply avoiding regulatory enforcement action and take appropriate steps to safeguard their systems and in turn

[3] *See* "UK Telco Fined for Cyber Breach: Lessons Learned" (October 2016), http://www.debevoise.com/~/media/files/insights/publications/2016/10/20161019_uk_telco_fined_for_cyber_breach_lessons_learned.pdf.

their wider business interests. Actively engaging with both existing and future Government guidance and information sharing initiatives can help businesses achieve this aim.

This client update was originally issued on February 6, 2017.

UK Government Launches Five Year National Cyber Security Strategy

On 1 November 2016, the UK Government issued its new National Cyber Security Strategy, outlining its goals for the next five years and committing £1.9 billion to combat cyber-threats. A link to the UK Government's Strategy can be found here.

Replacing the UK Government's 2011 National Cyber Security Strategy, the new Strategy aims to ensure that the UK remains "at the vanguard of the digital revolution" while protecting national interests, the UK economy and its citizens. The Strategy also reflects a global trend towards greater focus on businesses' cybersecurity controls. In particular, the UK Government will work with regulators, insurers and investors to compel businesses to manage cyber-risk effectively.

While acknowledging that it is impossible to eliminate cybersecurity risks entirely, the UK Government stresses the pervasive need for improved cybersecurity, not only in the public and private sectors but also on a collective and individual level. It notes that tackling cybersecurity threats "is a task for us all", including businesses, and calls for "whole-society capability" to address cyber-risk.

Businesses should, therefore, be mindful of the UK Government's Strategy and how it might impact them. One of the Strategy's key themes is collaboration and businesses will have the opportunity to work alongside the UK Government to ensure that their needs are met. For example, businesses will be able to benefit from Government resources such as threat intelligence from the National Cyber Security Centre which launched on 3 October 2016. The UK Government also commits to work closely with the private sector to

define how businesses should engage with Government when a cyber-incident occurs.

Notwithstanding this collaboration, the Strategy makes clear that ultimate responsibility for businesses' cybersecurity "sits with boards, owners and operators". The UK Government also stresses that it will use all available levers to ratchet up businesses' cybersecurity including the EU General Data Protection Regulation requirements which enter into force in May 2018.

Businesses should therefore ensure that they are ready to meet the UK Government's expectations and, in particular, become GDPR compliant if they are not already.

This client update was originally issued on November 2, 2016.

UK Telco Fined for Cyber Breach: Lessons Learned

NOTE: This article first appeared on the StrategicRISK website on 17 October 2016.

On 30 September 2016, the UK's Information Commissioner's Office ("ICO") fined TalkTalk Telecom Group plc a record £400,000 for data security failings that allowed a hacker to access almost 157,000 customers' personal information last year. The monetary penalty serves as an opportunity for companies to reassess their cybersecurity risk profile—particularly in the context of mergers, acquisitions and post-M&A integration—and ensure that their systems and controls meet regulators' latest expectations.

WHAT WENT WRONG?

In 2009, TalkTalk, the UK TV, broadband and telecoms provider, acquired the UK operations of the Italian telecoms operator, Tiscali. Unknown to TalkTalk, Tiscali had legacy webpages that allowed access to a customer database and which remained accessible via the internet post-acquisition.

The database was stored on an outdated version of MySQL, affected by a software bug for which a fix had been available since 2012. In October 2015, a hacker exploited this vulnerability on three legacy Tiscali webpages to access the database. The hacker acquired almost 157,000 customers' personal data such as their names, addresses, dates of birth, telephone numbers, email addresses and financial information.

The ICO fined TalkTalk for two breaches of the UK Data Protection Act 1998: First, for failing to take appropriate technical and organisational measures against the unauthorised or unlawful

processing of personal data. Second, for keeping customers' data for longer than was necessary for the purposes it had been collected.

While the ICO found that TalkTalk had not deliberately breached its obligations, its failings still represented a "serious oversight" which led the ICO to issue a record breaking £400,000 fine.

LESSONS LEARNED

The TalkTalk penalty is a timely reminder of the global trend of increasing regulatory scrutiny of businesses' cybersecurity posture. Companies can learn from TalkTalk's experience to better protect themselves. The following takeaways from the TalkTalk penalty notice may be helpful.

First, (re)identify your information architecture. Companies should know what data they hold and where and how. This is not a one-off task; companies should constantly monitor changes which may affect their data security requirements. By apparently failing to audit Tiscali's webpages either during pre-acquisition due diligence or following acquisition in 2009, TalkTalk left the door open for hackers six years later.

Businesses may, therefore, wish to identify ahead of time situations that might require a non-routine reassessment of their data architecture, such as acquiring another company, changing data hosting arrangements or retiring old IT systems.

Second, adopt tailored and proportionate protections. Not all data should necessarily be treated equally. Companies are well advised to determine which data assets are most critical, not only to the company itself, but also to its customers. For instance, the ICO said

TalkTalk ought reasonably to have known that failing to adequately protect the database could cause substantial damage to those whose data was stored on it.

A proportionate protection framework may enable a company to deploy resources where they are needed most and to use cybersecurity budgets more efficiently. In TalkTalk's case, the ICO emphasised that the fact that the customer database contained financial information heightened the need for robust technical and organisational safeguards. It found that TalkTalk overlooked the need to ensure that it had robust measures in place to protect such data, despite having the financial and staffing resources available to do so. Companies may, therefore, wish to differentiate between the types of data they hold, how each category is protected and how long each is kept to help minimise cybersecurity risk efficiently and in a risk-based manner.

Third, be proactive. While cyber threats are often asymmetric (you cannot control a hacker), businesses should consider whether they have adequate systems and controls in place which allow them to identify and monitor suspicious activity and discover vulnerabilities. This ranges from the high tech (*e.g.*, periodic penetration testing and real time data monitoring) to routine housekeeping (*e.g.*, enforcement of document retention policies that call for periodic purging of older data). The ICO penalised TalkTalk for not updating its database software to address a known vulnerability, in what it called an "ongoing contravention." It is therefore important that companies have ways to systematically pre-empt, identify and quickly resolve these sorts of issues.

Fourth, be ready to respond and remediate. Regulators do not expect perfection. Companies may, however, be cast as a villain, rather than a victim, if they are not prepared to deal with an attack quickly, effectively and transparently, with a focus on protection of consumers. The ICO recognised that TalkTalk had been the subject of a criminal attack as a mitigating factor in its decision to fine the company. The ICO also recognised, as mitigating factors, that TalkTalk took substantial remedial action, notifying affected customers and offering 12 months of free credit monitoring.

Companies generally are better placed to deal with a breach if they have a carefully crafted incident response plan in place ahead of time. By pre-emptively thinking about how and who will deal with incidents of varying degrees of severity, businesses can respond more quickly and more effectively when they arise. For example, knowing in advance what information you will need to give regulators, customers and the press (and who will give it) may help a business channel scarce resources in a time of crisis.

THE FUTURE

With regulators' ever-increasing focus on cybersecurity showing no signs of abating, companies should act now to ensure they have a robust framework to address cybersecurity risk. While some may see the TalkTalk fine as relatively lenient, the EU General Data Protection Regulation, which comes into force in May 2018, brings with it increased penalties of up to the greater of €20 million or 4% of global annual turnover for the preceding financial year.

Companies are likely, therefore, only to see the cost of noncompliance increase in the future. If applied to TalkTalk, for example, the new EU regime could have resulted in a monetary

penalty of more than £50 million, far exceeding the maximum £500,000 penalty it could have received at present. Businesses may, therefore, wish to act now, rather than pay the tariff later.

This client update was originally issued on October 19, 2016.

China's Network Security Law Takes Effect

On June 1, 2017, China's new Network Security Law (the "Law") officially came into force. When the Law was first passed in November 2016, we noted that this first-ever law devoted solely to cybersecurity in China would impose substantial obligations on businesses operating in China. Most significant were obligations of the operators of "critical information infrastructures" ("CII Operators") to store data within Mainland China, conduct security assessments for cross-border data transfer, and purchase only network products or services which have been subject to a security review.[1] We also noted that the Law potentially would affect multinationals' IT infrastructure and their ability to transfer data abroad.

At that time, there was significant doubt about the vague and broad terms of the Law, and some hope that these might be clarified by additional implementing regulations.[2] While the Law is now in effect, there has been little clarification, and one of the significant implementing regulations will not go into effect for another 18 months.

Earlier this year, the Cyberspace Administration of China ("CAC")—China's top internet regulator—released two implementing

---

1 Under the Law, CII Operators are defined as "entities involved in a wide range of sectors including public communication and information services, energy, transportation, water conservancy, finance, utilities and e-government" as well as "other important sectors and fields" whose damage could harm "national security, people's livelihoods and public interest." See Network Security Law, Art. 31.

2 "China Passes Network Security Law", Debevoise Client Update (Nov. 10, 2016), http://www.debevoise.com/insights/publications/2016/11/china-passes-network-security-law.

regulations related to the Law for public consultation. One of them, the *Measures for Security Review of Network Products and Services (For Trial Implementation)* ("Security Review Measures"), offers guidance on security standards, and outlines a government-led security review process to be implemented for certain network products and services.[3] The other regulation, the *Measures on Security Assessment of Cross-Border Data Transfer of Personal Information and Important Data* ("Data Transfer Measures"), governs cross-border data flow and delineates a security assessment process on transfer of data abroad.[4] Both the Data Transfer and the Security Measures were slated to take effect on June 1st, although many businesses which routinely transfer data abroad found both to be lacking in clarity.

Last month, a coalition of dozens of global business groups called on China to delay implementing the Law and regulations, complaining that the Law would hamper market access and conflict with World Trade Organization regulations. Subsequently, the CAC decided to delay implementation of the Data Transfer Measures until December 31, 2018. The Security Review Measures, however, became effective on June 1st.

---

[3] In February 2017, the first draft of the Security Review Measures was released for public comment. On May 2, 2017, the final version of the Measures was released, a copy of which in Chinese is available http://www.cac.gov.cn/2017-05/02/c_1120904567.htm.

[4] On April 11, 2017, the first draft of the Data Transfer Measures was released for public comment, a copy of which in Chinese is available at http://www.cac.gov.cn/2017-04/11/c_1120785691.htm. On May 19, 2017, the Cyberspace Administration of China ("CAC") invited international stakeholders to attend a seminar to discuss an updated version of the Data Transfer Measures. References here are made to this updated version of the Data Transfer Measures, although this version has not been official published yet.

SECURITY REVIEW MEASURES

The stated purpose of the Security Review Measures is to implement Article 35 of the Law, which requires CII Operators to ensure that "network products and services" they purchase have passed a "security review."

The network security review requirement focuses on whether the products and services are "secure and controllable." A number of specified risks must be assessed during the review—for example, the risk of products or services being unlawfully controlled, interfered with or otherwise hacked.[5] The CAC has set up a Cybersecurity Review Commission (the "Commission") responsible for adopting relevant policies relating to security reviews. A Cybersecurity Review Office will be set up to handle the actual review.[6] In addition, the Commission will assemble expert panels to assess security risks.[7] Specific review methods will include lab testing, on-site inspection, online monitoring, and background check.[8]

The Security Review Measures lay out general principles rather than specifying practical guidelines. For example, these Measures do not specify any timeframe for the review process, nor do they make it clear how the security risks will be assessed. Such lack of clarity provides substantial discretion to the regulators.

DRAFT DATA TRANSFER MEASURES

The Data Transfer Measures remain in the draft form issued on May 2, 2017. They are to be enforced from December 31, 2018. The Data

5 Security Review Measures, Art. 4.

6 Security Review Measures, Art. 5.

7 Security Review Measures, Art. 6.

8 Security Review Measures, Art. 3.

Transfer Measures aim to clarify the data localization and transfer provisions under the Law. Article 37 of the Law provides that CII Operators must store "personal information and important data" collected and generated during operation within Mainland China, and cross-border data transfer will be subject to a "security assessment."

The Data Transfer Measures expand the scope of "security assessment" under the Law to cover not only CII Operators, but also general "Network Operators."[9] "Network Operators" are defined under the Law as "owners or managers of a network, or network service providers,"[10] terms so broad they could cover virtually every entity that uses networks to conduct business, regardless of the industrial sector. This means, for example, that a company merely operating a local area network to collect employee information may also need to conduct a security assessment for intra-company data transfer abroad.

Two types of data will be subject to the security assessment requirement: "personal information" and "important data." "Personal information" refers to information that can be used to identify a person's identity alone or in combination with other information, such as name, date of birth, identity document number, etc.[11] "Important data" does not mean data that are important to the corporation, but those "closely related to national security, economic development, and social and public interests".[12]

---

9 Draft Data Transfer Rules, Art. 2.

10 Network Security Law, Art. 76(3).

11 Data Transfer Measures, Art.15; Network Security Law, Art. 76(5).

12 Data Transfer Measures, Art. 15.

The Data Transfer Measures provides for two types of assessment processes: self-assessment and regulator assessment. In general, Network Operators are obliged to conduct security assessments for their cross-border data transfer.[13] However, an industry regulator will conduct the security assessment if the transfer contains a "huge" amount of personal information (defined as relating to over 500,000 Chinese citizens), or if the transfer involves data related to sensitive matters (*e.g.*, nuclear facilities, national defense, marine environment, etc.) or involves data related to cybersecurity information of CII Operators, or if the transfer involves other data that may potentially affect national security and public interests.[14] The Data Transfer Measures also lay out the substantive criteria applied to both self-assessment and regulator assessment, including the aspects to assess (for example, amount, scope, type, level of sensitivity of personal information involved), as well as the circumstances under which cross-border transfer will be prohibited (for example, the transfer poses risks to China's national security or public interests).[15]

Notably, the Data Transfer Measures offer strong protection on personal information. According to Article 4 of the Data Transfer Measures, to transfer personal information abroad, the data subject must be notified of "the purpose, scope, type and the country or region where the recipient is located," and consent to the transfer. The only exception to this requirement is when urgent circumstances occur under which the security of citizens' lives and properties are endangered. The Data Transfer Measures also

---

13 Data Transfer Measures, Art. 6.

14 Data Transfer Measures, Art. 7.

15 Data Transfer Measures, Arts. 8 and 9.

emphasize that absent the data subject's consent, no cross-border transfer of personal information is allowed.[16] The lack of any stated exceptions to this rule, combined with the broad definition of "personal information," would appear to make any data transfer particularly burdensome. This breadth will hopefully be addressed before the Data Transfer Measures take effect in 18 months.

LOOKING FORWARD

Although the Law and the Security Review Measures have already taken effect, there is a lack of clarity as to how to comply with both documents. It is unclear as to when the Draft Data Transfer Measures will be officially adopted and whether they will be adopted in the current near final version. It is also unknown what the regulator's enforcement priorities will be or exactly how security reviews will be carried out, although businesses that operate in or supply critical industries should be more alert than others.

It is to be hoped that additional implementing regulations or guidelines will be issued in the near future. In the meantime, corporations subject to the Law can consider:

- Continuing to work with Chambers of Commerce and other business groups in China to encourage greater clarity;
- Evaluating whether they meet the definition of CII Operators, based on the business nature, the industries that they supply, and the nature and amount of data collected and processed during business operation;
- Reviewing current IT infrastructure deployments and data compliance programs, and assessing whether they could comply

[16] Data Transfer Measures, Art. 9(2).

with the requirements on data localization, cross-border data transfer, and product or service security review;
- Consulting with legal professionals to identify improvements necessary to increase cyber compliance; and
- Planning ahead for potential interaction with regulators, and mapping out crisis management strategies.

This client update was originally issued on June 9, 2017.

China Passes Network Security Law

On November 7, 2016, the Standing Committee of the National People's Congress of China adopted the Network Security Law, which will come into force on June 1, 2017.[1] The country's first-ever law devoted solely to cybersecurity:

- codifies a variety of cyber-crimes such as illegally obtaining or selling personal information,[2] disseminating malicious software or "prohibited information,"[3] and online fraud;[4]
- imposes obligations on "Network Operators" with regard to the protection of personal information, content monitoring for "prohibited information," and cooperation with the authorities;
- imposes additional data localization, data transfer restrictions, and cybersecurity obligations on "Critical Information Infrastructure Operators"; and
- envisions pre-approval of "critical network equipment" and "specialized cyber-security products" and security screening for "network products or services."

Violations of the obligations and restrictions in the law can result in administrative penalties and fines, including suspension or revocation of a business license, as well as fines and other penalties for responsible persons.

---

1 National People's Congress of China, "Network Security Law of the People's Republic of China" [in Chinese: Wang Luo An Quan Fa], XinhuaNet (Nov.11, 2015), http://news.xinhuanet.com/legal/2016-11/07/c_1119867015.htm.

2 Network Security Law, Art. 44.

3 Network Security Law, Art. 48.

4 Network Security Law, Art. 46.

The scope and impact of the Network Security Law on multinational corporations will depend on additional implementing regulations further clarifying the vague terms in the law. As passed, however, the Network Security Law has the potential to severely restrict businesses' ability to transfer and store data abroad as well as restricting the availability of "critical network equipment" and "specialized cyber-security products" in China. These restrictions could require significant alterations or upgrades to existing or future IT infrastructure in China.

NETWORK OPERATORS

"Network Operators" are defined as "owners and managers of networks and network service providers."[5] Based on similar terms in other laws,[6] a "Network Operator" could include not only telecommunication operators and internet service providers, but also any provider of online information and services, including search engines, video websites, email service providers, e-commerce platforms, mobile messaging tools, social community operators, and websites of corporations and non-profit organizations.

---

5 Network Security Law, Art. 76 (3).

6 For example, "Provisions on Technical Measures for the Internet Security Protection" (effective on Mar. 1, 2006), Art. 18, which states, "for the purposes of these Provisions, Internet service providers shall mean the organizations that provide users with Internet access services, Internet data center services, Internet information services, and Internet Web services." For another example, "Administrative Measures on Internet Information Services" (effective on Sep. 25, 2000), Arts. 2 & 3, which defines "Internet information service" to be "service activities of providing information to online users via the Internet," including both "profit-making" and "non-profit-making" Internet information services.

Data Collection and Processing

The Network Security Law integrates scattered provisions of previous regulations[7] into a set of rules governing the collection of personal information[8] by Network Operators.

Network Operators must establish and improve their user information protection system and keep their user information strictly confidential.[9] At the time of collection, Network Operators must expressly state the purposes, methods, and scope of data collection and obtain the individual's consent. Only relevant personal information may be collected or used.[10] The Network Security Law does not specify what form of consent is acceptable. Without the consent of the user, Network Operators are prohibited from providing the user's personal information to any third party, unless redacted to remove personally identifiable information.[11] In the event of a breach or other improper transfer, Network Operators must immediately take remedial measures, and notify the affected

---

7 For example, Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection (effective on Dec. 28, 2012), Art.7; Provisions on Protecting the Personal Information of Telecommunications and Internet Users (effective on Sep. 1, 2013), Art. 9.

8 Personal information refers to "information that can be used to identify an individual when used either independently or in combination with other information, including but not limited to an individual's name, date of birth, identification number, biometric information, address, and phone numbers." *See* Network Security Law, Art. 76 (5).

9 Network Security Law, Art. 40.

10 Network Security Law, Art. 41.

11 Network Security Law, Art. 42.

users and report to the competent authorities in a "timely" manner.[12] "Timely" is not defined in the law.

Content Monitoring

Under Article 47, Network Operators have a duty to monitor the information published by their users. Upon becoming aware of the publication or transmission of "prohibited information," Network Operators must promptly stop transmitting the information and prevent its spread. Network Operators are also required to maintain records and report incidents to the competent authorities.[13] Based on earlier laws and regulations,[14] "prohibited information" includes a wide variety of political and religious speech, other speech that disturbs social stability, pornography and speech that encourages other illegal behavior, slander and other information that damages the lawful rights of third parties, as well as any information that is otherwise prohibited by law or administrative regulation.

Cooperation with Authorities

Article 28 of the Network Security Law imposes duties (echoing those imposed by the Anti-Terrorism Law) on network operators to provide technical support and assistance to public security and national security agencies in national security and criminal investigations. Although technical support and assistance is not defined in the Network Security Law, under the Anti-Terrorism Law,

---

12 Network Security Law, Art. 42.

13 Network Security Law, Art. 47.

14 For example, Administrative Measures for Protection of the Security of International Internetworking of Computer Information Networks (Dec. 30, 1997), Art. 5; Administrative Measures for Internet Information Services (effective on Sep. 25, 2000), Art. 15; Telecommunication Regulations (effective on Sep. 25, 2000), Art. 57; Anti-Terrorism Law (effective on Jan. 1, 2016), Art. 19.

this support would require providing "technical interfaces, decryption and other technical support and assistance" to security agencies.[15] The Network Security Law does not specify any process that the agencies must go through prior to requesting cooperation.

ADDITIONAL OBLIGATIONS OF CRITICAL INFORMATION INFRASTRUCTURE OPERATORS

"Critical Information Infrastructure Operators" are defined as entities involved in a wide range of sectors including public communication and information services, energy, transportation, water conservancy, finance, utilities and e commerce.[16] The definition also includes a catch-all category "other important sectors and fields." Moreover, the detailed scope and protective measures relating to critical information infrastructure is explicitly left to future regulation by the State Council.[17] The impact of the Network Security Law on foreign businesses will largely be determined by how narrow or broad these future regulations are.

Data Localization Requirement

The Network Security Law imposes a data localization obligation on Critical Information Infrastructure Operators. Article 37 of the Law states,

> Personal information and important business data collected and generated in the operation of critical information infrastructures operators within the territory of the People's Republic of China shall be stored within the territory. Where it is necessary to provide

15 Anti-Terrorism Law, Art. 18.

16 Network Security Law, Art. 31.

17 Network Security Law, Art. 31.

> such information and data abroad due to business needs, security assessment shall be carried out according to the measures formulated by the national Internet information department in conjunction with the relevant departments of the State Council; if there are other provisions in laws and regulations, those provisions shall prevail.

The broad wording of Article 37 requires the adoption of detailed implementing rules. Most significantly, "important business data" is not defined, making it difficult to determine what must be stored in China. It also remains to be seen: which entity will conduct the security assessment prior to "provision of information abroad"; how onerous that assessment is likely to be; and whether such an assessment will apply only to individual transfers, or whether it could permit routine transfer—equivalent to the storage of data abroad.

Ongoing Cybersecurity Obligations

The Network Security Law also introduces a new set of security protection obligations applicable to Critical Information Infrastructure Operators, including: (i) setting up special security management departments and responsible persons (and conducting background checks of such responsible persons),[18] (ii) conducting training on cybersecurity on a regular basis,[19] and (iii) carrying out testing and evaluation of the security and potential risks of its network.[20]

---

[18] Network Security Law, Art. 34 (1).

[19] Network Security Law, Art. 34 (2).

[20] Network Security Law, Art. 38.

Technology Regulation

Article 23 of the law requires certification and approval of "critical network equipment" and "specialized cyber-security products" by a "qualified institution" not defined in the law. While the purpose of certification is to ensure that such technology is "secure and reliable," in practice, it is likely to restrict the availability of such equipment and products to a preapproved list which could result in: (i) currently existing equipment and products (especially foreign equipment and products) becoming unavailable if it is not certified and/or (ii) a delay in the ability of multinationals doing business in China to implement global technology upgrades pending certification. Obviously, Article 23 also raises concerns about the possibility of discrimination against foreign technology companies in the certification process.

In addition to the certification requirement in Article 23, Article 35 of the law restricts how Critical Information Infrastructures Operators may store data. Specifically, when a Critical Information Infrastructures Operator purchases "network products or services" that may affect or involve national security, the product or service will be subject to a security review jointly arranged by the National Internet Information Department and the relevant departments of the State Council.[21]

This client update was originally issued on November 10, 2016.

[21] Network Security Law, Art. 35.

SFC Cybersecurity Review of Internet/Mobile Trading Systems

On 13 October 2016, the Hong Kong Securities and Futures Commission ("SFC") announced a review of the cybersecurity preparedness, compliance and resilience of brokers' internet/mobile trading systems.

The review follows 16 reported hacking incidents which involved 7 securities brokers and total unauthorized trades in excess of HK$100 million.

The review will comprise three components:

- A questionnaire provided to a mix of small to medium sized securities and futures brokers as well as leveraged foreign exchange traders. The primary objective is to assess the cybersecurity aspects of internet/mobile trading systems.
- Onsite inspections of selected brokers for a deep dive review of their information technology and other related management controls and an assessment of their design and effectiveness in preventing and detecting cyberattacks.
- Benchmarking the SFC regulatory requirements and market practices in Hong Kong against requirements of major financial services regulators and other relevant market practices in Hong Kong or elsewhere.

The findings of this review will be used by the SFC to further develop policy to improve overall cybersecurity resilience in the markets.

Cybersecurity management is a key priority for the SFC's supervision of licensed corporations ("LCs") and the SFC has promulgated a number of Circulars setting out in detail the cybersecurity controls which it expects LCs to implement. In particular, in addition to controls for the detection and prevention of cyberattacks, the SFC also expects LCs to have a written contingency plan for dealing with cyberattacks when they happen. The SFC has urged LCs to review and enhance their cybersecurity controls in light of the latest incidents. LCs which fail to implement adequate cybersecurity controls risk enforcement action.

The SFC's activities closely mirror steps other regulators worldwide have taken with respect to cybersecurity. The U.S. Securities and Exchange Commission ("SEC") Office of Compliance Inspections and Examinations ("OCIE"), for instance, conducted a similar sweep, resulting in a published report in February 2015. The SEC has since brought three actions against registered investment advisors for cybersecurity lapses. Similarly, the New York Department of Financial Services last month proposed stringent cybersecurity regulations for regulated banks (including foreign banks operating in New York) and insurance companies.

The UK Financial Conduct Authority ("FCA") is also crystallizing its stance on cybersecurity and has publically stated that all UK regulated entities should address cybersecurity threats, irrespective of their size or services offered. In nonbinding comments, the FCA has also signaled that firms should have a "security culture" that permeates from the board to every employee, as well as calling for greater information sharing both with the regulator and between financial institutions. While the FCA is yet to issue specific cybersecurity requirements, it is clear that it will use the existing

regulatory regime to enforce against firms which fail to implement adequate systems and controls to address cyber risk or report significant incidents when they occur.

This client update was originally issued on 17 October 2016.

New Regulation of Online Cinemas in Russia

On May 1, 2017, Federal Law No. 87-FZ on Amendments to the Federal Law on Information, Information Technologies and Protection of Information and Certain Laws of the Russian Federation ("Law No. 87") was adopted. Law No. 87 is mainly targeted at providers which stream videos via over-the-top (OTT)[1] platforms (online-cinemas)[2] and other providers distributing digital videos to Russian customers. It is not targeted at:

- providers which allow users to post their own videos;[3]
- search engines[4] and
- network mass media.[5]

Law No. 87 directly affects such businesses by restricting foreign participation and imposing new obligations on their owners. Law No. 87 comes into force on July 1, 2017.

The main provisions of Law No. 87 are described in more detail below.

ONLINE-CINEMA AS AUDIOVISUAL RESOURCE

As of July 1, 2017, an audiovisual resource will have to be included in the register of audiovisual resources (the "Register") maintained by

---

1 OTT content is delivered over the Internet without the involvement of a multiple-system operator in the control over or distribution of the content.

2 *E.g.*, Netflix, iVI, MegaFon.TV.

3 *E.g.*, YouTube, RuTube.

4 *E.g.*, Google, Yandex.

5 *E.g.*, Tvrain.ru.

the Federal Service for Oversight in the Sphere of Communications, Information Technologies and Mass Media ("Roskomnadzor").

Online-cinema will qualify as an audiovisual resource if it is a website, webpage, information system or software which is used (i) to form and/or organize the online distribution of fee-based audiovisual products,[6] or (ii) for viewing advertisements, if such advertisements are targeted at consumers resident in Russia, provided that more than 100,000 Internet users resident in Russia access such online-cinema daily.

An online-cinema will not qualify as an audiovisual resource if it is a network mass media or an information resource providing access mainly to content posted by users.

If fewer than 100,000 Internet users access an audiovisual resource daily over a period of three months, its owner can apply to Roskomnadzor for its removal from the Register. If this threshold is not met during six consequent months, Roskomnadzor will exclude it from the Register on its own.

RESTRICTIONS ON FOREIGN PARTICIPATION IN ONLINE-CINEMAS

Only a Russian company or a Russian citizen without foreign citizenship can own online-cinema which qualifies as an audiovisual resource ("AR"):

[6] According to Article 1263 of the Civil Code of the Russian Federation, an audiovisual product is a product consisting of a fixed series of interconnected images (with or without sound) and intended for visual and acoustic (if applicable) perception with respective technical equipment. Audiovisual products include films, TV and video films and other similar products.

- foreign[7] participation in a Russian company which owns AR is restricted as follows: a 20% stake[8] in the charter capital of the AR owner for Foreigners who own audiovisual distribution products resource for which Russian subscribers constitute more than 50% of its total audience; or
- subject to governmental commission clearance -a more than 20% stake in the charter capital of the AR owner for Foreigners who own audiovisual distribution products resource for which Russian subscribers constitute less than 50% of its total audience; the governmental commission will only approve the Foreigner's acquisition of ownership, control or management of more than 20% of the charter capital of the AR owner if it promotes the development of the market of audiovisual resources in Russia.

DUTIES OF AN OWNER OF AUDIOVISUAL RESOURCES

An AR owner must:

- not use the AR for committing a crime, for the distribution of information constituting a protected secret (*e.g.*, a state secret), distribution of materials encouraging terrorist attacks or publicly justifying them, other extremist materials, materials encouraging pornography, cruelty or violence, and materials containing taboo language;
- classify information intended for children before the start of its distribution and label it accordingly;

---

7 A foreign participant is: a foreign state; an international organization; an entity controlled by a foreign state or international organization; a foreign company; a Russian company with more than 20% foreign participation; a foreign citizen; a stateless person or a Russian citizen with citizenship of another state; and affiliates of persons listed above (each - a "Foreigner" and together - "Foreigners").

8 Including ownership, management or control over such stake.

- comply with restrictions and prohibitions provided by legislation on elections and referenda;
- comply with requirements for the distribution of mass media;[9]
- avoid broadcasting TV channels or TV programs not registered as mass media in Russia;
- provide e-mail addresses or web-forms and make available its name and address for legal communication purposes; and
- install one of the types of software offered by Roskomnadzor for calculating the number of subscribers to the AR.

If an AR posts information that is prohibited for distribution in Russia, Roskomnadzor will issue a compliance order to its owner. If the owner repeatedly, within a year, fails to comply with Roskomnadzor's compliance order or fails to provide documents confirming compliance with restrictions for foreign participation or to comply with these restrictions, Roskomnadzor will apply to the court to restrict access to the AR and may subsequently block it. An AR owner (if it is a company) may also be subject to a fine of up to RUB 3,000,000 (approx. USD 52,500), and its officers up to RUB 700,000 (approx. USD 12,246) (depending on the particular violation).

This client update was originally issued on 2 June 2017.

[9] Such requirements are established by the Law of the Russian Federation No. 2124-1 on Mass Media dated December 27, 1991 and, *inter alia*, provide for the obligation to give output details for each program.

Russian Data Protection Developments: Localization, Messengers and Data Transfer

This spring the following issues were on the radar of the Russian data protection regulators:[1]

- messengers' compliance with the requirements of internet data facilitators;
- Twitter localization in Russia; and
- the definition of cross-border transfer of personal data.[2]

MESSENGERS: INTERNET DATA FACILITATORS' COMPLIANCE

Messengers facilitate exchange of electronic messages between their users via the Internet without control of a telecom carrier. According to Article 10.1 of the Information Law,[3] they qualify as Internet data facilitators as they operate through information systems and/or software intended and/or used for the reception, transfer, delivery and/or processing of the electronic messages of Internet users. As a result all messengers have to:

- notify Roskomnadzor on the start of their operations in Russia;[4]
- store information about their subscribers in Russia, as well as any information on the receipt, transfer, delivery and/or processing of

---

1 The Federal Service for Oversight in the Sphere of Communications, Information Technologies and Mass Media ("Roskomnadzor") and the Ministry of Communications and Mass Media.

2 Article 3 of the Federal Law No. 152-FZ on Personal Data dated July 27, 2006 (the "Personal Data Law").

3 Federal Law No. 149-FZ on Information, Information Technology and Protection of Information dated July 27, 2006 (the "Information Law").

4 The notification is not mandatory but Roskomnadzor may require the messenger to provide such notification if it is not done.

voicemail, written text, images, sounds, video, etc. of such subscribers for one year after the respective actions are completed and provide this information to any governmental investigative or state security authorities upon their justified request;
- ensure that the equipment and software used allow governmental investigative or state security authorities to perform their functions (*i.e.*, install specific equipment and software which enables the respective governmental authorities to collect and analyze information required for the performance of their functions) and keep the respective information confidential; and
- provide the Federal Security Service with information required for decoding the electronic messages of its subscribers if the respective service enables such messages' additional coding.

Failure to comply with these requirements may lead to an administrative fine in the amount of up to RUB 1,000,000 (approx. USD 17,500) for legal entities and up to RUB 50,000 (approx. USD 875) for officers.[5] Failure to eliminate the violations may lead to the blocking of the messenger per court or authorized administrative body decision until it cures the violation.

In the framework of its routine activity on maintenance of the Register of Internet Data Facilitators ("Register"), Roskomnadzor requested that several messengers provide information for the Register. Such steps were also aimed at facilitating the messengers' further communication with Roskomnadzor. Several services, including Vimeo, Opera and WeChat, complied with Roskomnadzor'

[5] Article 13.31 of the Administrative Offences Code of the Russian Federation.

requirement, but some others, such as Blackberry Messenger, Imo, Line and VChat, refused to do so.

As a result, in May 2017, Roskomnadzor blocked Blackberry Messenger, Imo, Line and VChat in Russia. The blocked services can challenge Roskomnadzor's decision on blocking in court.[6] As of today there is no publicly available information on such challenge and these messengers remain blocked.

TWITTER LOCALIZATION IN RUSSIA

Under Article 18 of the Personal Data Law, recording, systematization, accumulation, storage, updating (renewal, amending) and extraction of the personal data of Russian citizens must be done only through databases located in Russia. Personal data processors' failure to comply with this requirement may result in the blocking of the respective resources upon Roskomnadzor's request on the basis of a court decision.

As of now Twitter is not registered in Russia. At the beginning of 2016, Roskomnadzor determined that Twitter processed the data of Russian citizens and targeted Russia,[7] and consequently was subject to Russian personal data law requirements, including requirements on localization and provision of non-English-speaking Russian customers with terms of use and a confidentiality policy in Russian. This did not, however, result in the blocking of Twitter,[8] and in April 2017, Twitter notified Roskomnadzor that it will transfer personal

---

6 Article 218 of the Administrative Proceedings Code of the Russian Federation.

7 Twitter's website and application for smartphones had a Russian version.

8 Although a similar violation resulted in blocking of LinkedIn in 2016.

data of its Russian users to Russian servers by mid-2018. The absence of blocking and a substantial grace period for compliance with the localization requirement might have been a result of Twitter's cooperation and interaction with Roskomnadzor. In addition, the blocking might have had a significant negative social impact. Twitter has a monthly audience of more than seven million in Russia and is used by some government officials to reach audiences quickly. This case indicates that Roskomnadzor has the discretion to commence blocking proceedings and may not block resources that cooperate and undertake to comply with Russian law requirements.

CROSS-BORDER TRANSFER OF DATA

As currently defined in the Personal Data Law, the cross-border transfer of data is a transfer of personal data to the territory of a foreign state to:

- a foreign state authority;
- a foreign individual; or
- a foreign legal entity.[9]

The definition does not cover transfers of personal data to Russian companies' or individuals' servers located abroad. In order to eliminate this loophole, the Ministry of Communications and Mass Media has proposed amending this definition to specify that any transfer of data to the territory of a foreign state qualifies as a cross-border transfer. Such qualification will require a written consent of the personal data subject for the transfer of personal data to a foreign state even within one personal data processor if the respective

[9] Article 3 of the Personal Data Law.

foreign state does not ensure adequate protection of the rights of the personal data subjects.

The proposed amendments are currently undergoing public discussion.[10]

This client update was originally issued on May 31, 2017.

[10] Full text of amendments is not yet available (http://regulation.gov.ru/projects#npa=64389.)

Russia 2016: Personal Data & Cybersecurity

2016 was a notable year in Russia for the extension of control over, and further clarification of, data localization requirements;[1] establishment of a strategy for the further development of personal data legislation and an increase in attention to cybersecurity issues.

PERSONAL DATA LOCALIZATION: FIRST OUTCOME

On September 1, 2016, the Federal Service for Oversight in the Sphere of Communications, Information Technologies and Mass Media of the Russian Federation ("Roskomnadzor") published the first results of the application of personal data localization requirements, which demonstrated the following:

- 161 Internet resources were included on the Register of Violators of the Rights of Personal Data Subjects (the "Register") and blocked; and
- amongst all of Roskomnadzor's inspections in the sphere of personal data, the violations of personal data localization requirements amounted to 1.3 percent (23 violations out of 1822).

A warning order by Roskomnadzor to rectify the violation was the main penalty for violation of the data localization requirements.

[1] The data localization requirement was introduced by Federal Law No. 242-FZ on Amendments to Certain Legislative Acts of the Russian Federation with Regard to Specifying the Procedure for the Processing of Personal Data in Data Telecommunications Networks dated July 21, 2014 ("Law No. 242") and entered into force on September 1, 2015. It provides that recording, systematization, accumulation, storage, updating (renewal, amending) and extraction of personal data of Russian citizens can be done only through databases located in Russia ("personal data localization").

Certain companies have managed to remedy violations after the receipt of a warning order by Roskomnadzor.

PERSONAL DATA LOCALIZATION: CLARIFICATIONS

On November 9, 2016, Roskomnadzor published commentary clarifying certain aspects of the personal data localization requirements. Although the commentary does not have a binding effect on personal data operators, Roskomnadzor may take the commentary into consideration during its inspections and when deciding whether a violation has occurred.

Restricting Access to Internet Resources Used for the Processing of Personal Data

Under the Personal Data Law,[2] access to Internet resources is restricted on the basis of a court decision. Thus, a personal data operator has an opportunity to provide evidence that it processes personal data in accordance with the requirements of the law.

The procedure restricting access to Internet resources can be initiated as a result of the following violations[3] of the Personal Data Law:

- personal data is accumulated in foreign databases;
- personal data is processed without their subject's consent;
- public access to publicly available personal data is provided in contradiction with the original scope and purposes of accumulation of such personal data; or

[2] Federal Law No. 152-FZ on Personal Data dated July 27, 2006 (the "Personal Data Law").

[3] The list is not exhaustive.

- a personal data operator fails to make its policy on the processing of personal data publicly available on the Internet.

Roskomnadzor uses publicly available WHOIS-service to determine an entity against which a claim restricting access is brought.[4]

Roskomnadzor noted that termination of operation of Internet resources does not qualify as a ground for its exclusion from the Register. An Internet resource can be excluded from the Register when the violation was cured or the court set aside the respective Roskomnadzor's decision on inclusion of an Internet resource on the Register.

Clarification of Applicable Terms

Roskomnadzor explained the meaning of certain terms used in the Personal Data Law, including the following:

- "*database*" means any systematization of personal data, irrespective of their tangible media and processing facilities (*e.g.*, archives, electronic databases, MS Word and MS Excel documents, etc.); transfer of personal data from paper documents to an electronic database is considered as a single process, which shall be effected in Russia (*e.g.*, if a personal data operator accumulates personal data in paper documents in Russia and then transfers them to a foreign electronic database, the operator violates the Personal Data Law);

[4] WHOIS allows for identification of the owner of a domain name. Identification through WHOIS of an entity violating the personal data localization requirements for the purpose of restricting access to Internet resources was held to be legal in several judgments of appellate courts and courts of cassation.

- "*collection of personal data*" means receipt of personal data directly from the subject of personal data; this term should be distinguished from the transfer of personal data for further processing;
- the law does not divide "*storage of personal data*" into permanent storage and temporary storage; use of such specifications in the personal data processing consent violates the law.

Cross-Border Transfer of Personal Data

The requirements on personal data localization do not impose any additional restrictions on cross-border transfer of personal data located in Russia. However, any update of personal data must be done in a database located in Russia first, and only afterwards can such data be transferred abroad. Parallel input of personal data in a Russian and a foreign database contradicts the Personal Data Law.

LINKEDIN CASE

In 2016, access to the LinkedIn[5] Websites[6] was restricted for persons using Russian IP addresses.[7] The decision to block the LinkedIn Websites was based, among other things, on the failure by LinkedIn to comply with the data localization requirements and to obtain the consent of the relevant citizens for the processing of their personal data by LinkedIn.

---

5 LinkedIn Corporation ("LinkedIn").

6 Access is restricted to the domain names, URLs and network addresses of the following websites: http://www.linkedin.com and http://linkedin.com (the "LinkedIn Websites").

7 Based on the publicly available information, LinkedIn met with Roskomnadzor on December 8, 2016 in order to discuss Roskomnadzor's localization request, in particular, reasonable timing for localization. In January 2017, Apple and Google removed the LinkedIn application from their Russian application stores following a demand by Roskomnadzor.

To demonstrate the practicalities of the case, its details and background are set forth in Annex 1 to this update.

STRATEGY FOR PROTECTING RIGHTS OF PERSONAL DATA SUBJECTS

On March 31, 2016, Roskomnadzor adopted the Strategy for Institutional Development and Public Activities in Respect of the Protection of Rights of Personal Data Subjects to 2020 (the "Strategy"). The provisions of the Strategy are not binding, and their main goal is to set a roadmap for the future legislative and law enforcement activities of Roskomnadzor.

The Strategy promotes:

- self-regulation of the processing of personal data;
- consideration of industry specifics influencing the processing of personal data;
- increase of Roskomnadzor's public activity (*e.g.*, joint projects with professional communities of personal data operators); and
- transparency of activities aimed at strengthening personal data protection.

Basic actions provided by the Strategy include, among other things:

- creation of incentives for compliance with personal data legislation and improvement of existing regulatory mechanisms (which is expected to result in a decrease in personal data violations by 30 percent); and
- improvement of law enforcement and methodological instruments (which is expected to result in an annual decrease in the number of identified violations by 2 percent).

BILLS ON SECURITY OF RUSSIAN CRITICAL INFORMATION INFRASTRUCTURE

On December 6, 2016, Bill No. 47571-7 on the Security of the Critical Information Infrastructure in the Russian Federation and the related Bills No. 47591-7 and No. 47579-7 amending certain legislative acts of the Russian Federation in accordance with Bill No. 47571-7 (the "Bills")[8] were submitted to the State Duma of the Russian Federation.

The Bills establish basic principles for ensuring the security of Russian critical information infrastructure ("CII"),[9] and define the rights, duties and responsibilities of persons owning or otherwise legally holding CII facilities and telecom and information system operators supporting the interconnection of such facilities.

The Bills propose, among other things, the following:

- that a special register of significant CII facilities be created to ensure security of such CII facilities;
- that CII owners (including entities legally holding CII facilities) be required to report cyber incidents and assist the respective

---

8 For additional information on the Bills, please refer to:

http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=47571-7&02,
http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=47579-7&02,
http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=47591-7&02.

9 According to Bill No. 47571-7, CII facilities include, among other things, networks, information and telecom systems of government bodies, and networks, information and telecom systems operating in the defense, healthcare, transport, banking spheres, energy, fuel, nuclear, mining, metallurgical, chemical, space-rocket industries.

authorities in detecting and preventing cyberattacks, eliminating their consequences and determining the causes and circumstances contributing to such cyber incidents;
- that the criminal liability for improper interference with Russian CII (including creation and/or distribution of software or computer information deliberately designed for improper interference with Russian CII or unauthorized access to protected computer information stored in Russian CII) be set forth in Chapter 28 of the Criminal Code of the Russian Federation addressing cybercrime, with the maximum penalties, depending on the wrongdoing, being a criminal fine of up to RUB 2 million (approx. USD 33,333) or imprisonment for up to 10 years; and
- that the list of information classified as state secrets be amended to include information on the security measures in respect of CII facilities falling within one of the significance categories and information on the evaluation of the level of protection of Russian CII.

On January 27, 2017, the Russian State Duma passed the Bills in the first reading.

ACTIVITIES OF THE CENTRAL BANK OF RUSSIA

On April 11, 2016, the Central Bank of Russia issued Recommendations in the Sphere of Standardization for the Maintenance of Information Security of Institutions of the Banking System of the Russian Federation with regard to prevention of data leaks.

The document sets forth, among other things:

- measures recommended for adoption in order to prevent possible leaks of confidential information and recommendations with regard to the implementation of such measures;
- recommendations for the maintenance of the necessary and adequate level of monitoring and control of possible leakage channels; and
- types of data recommended for inclusion in the category of confidential information.

Moreover, in 2016, the Central Bank of Russia put forward two significant initiatives:

- to develop remedial actions in respect of banks with low information security levels (specific measures to be specified); and
- starting from 2017, to evaluate and develop regulations addressing remote banking services (in particular, to run an overall security check of online banking services for individuals and remote payment services for legal entities, introduce certification of such remote services for compliance with information security requirements, lay down requirements for such remote banking services and adopt the above requirements as national standards).

Particular documents supporting these initiatives of the Central Bank of Russia are under development.

We anticipate further development in the sphere of personal data protection and localization, as well as some initiatives regarding cybersecurity issues by the Russian banking community.

ANNEX 1

LINKEDIN CASE

Roskomnadzor's Claim

On June 16, 2016, Roskomnadzor filed a lawsuit against LinkedIn in the Taganskiy District Court of Moscow claiming that the operations of the LinkedIn Websites on the collection, use and storage of personal data of Russian citizens were illegal. Roskomnadzor also moved to include the LinkedIn Websites on the Register.

Roskomnadzor used the following arguments:

- LinkedIn failed to localize the processing of personal data in Russia as required by the Personal Data Law,[10] which provides that as a general rule, when collecting personal data (including through the Internet), an operator of personal data must procure that the recording, systematization, accumulation, storage, updating and extraction of personal data of Russian citizens be performed through a database located in Russia;
- LinkedIn did not obtain the consent of particular individuals to process their personal data in violation of the Personal Data Law,[11] because by synchronizing with users' e-mails and devices, LinkedIn also collected and processed the data of individuals who were neither "members" nor "visitors" of the relevant websites and, in Roskomnadzor's view, were not covered by LinkedIn's User Agreement or other documents; and

10 Art. 18, par. 5 of the Personal Data Law.

11 Art. 6, par. 1 of the Personal Data Law.

- according to the information from the LinkedIn Websites, LinkedIn, located outside of Russia, is responsible for the services of the website "linkedin.com"; moreover, this legal entity is the administrator of the domain name of the website "linkedin.com", and therefore, this entity was considered as the defendant.

At that stage, LinkedIn neither participated in the court proceedings nor sent a defense.

On August 4, 2016, the Taganskiy District Court of Moscow, having taken into account that LinkedIn's activities on the organization of personal data collection were purposeful, issued a judgment against LinkedIn and declared that LinkedIn violated the Personal Data Law and the respective privacy rights of Russian citizens.

As a result, Roskomnadzor included the LinkedIn Websites in the Register and, consequently, access to the LinkedIn Websites was restricted.

LinkedIn's Appeal Against the Judgment

LinkedIn appealed the judgment of the Taganskiy District Court of Moscow to the Moscow City Court, and claimed, among other things, that:

- the Roskomnadzor lawsuit was brought against the wrong legal entity, since LinkedIn Ireland Unlimited Company is processing the personal data of individuals residing outside of the United States, and not LinkedIn Corporation;[12]

[12] Par. 1.2 of LinkedIn's User Agreement as of October 23, 2014 provides that if an individual resides outside of the United States, then the agreement is entered into by LinkedIn Ireland Unlimited Company and the respective

- the provisions of the Russian legislation were not applicable to foreign companies;
- there was no violation of the rights of personal data subjects, as the complaints of Russian citizens with respect to the LinkedIn Websites were not provided; and
- LinkedIn was not duly notified about the time and place of the hearing in the court of first instance.

On November 10, 2016, the Moscow City Court dismissed LinkedIn arguments and upheld the judgment of the Taganskiy District Court of Moscow.

Roskomnadzor's position supported by the Moscow City Court was based, in particular, on the following arguments:

- LinkedIn is the operator of personal data responsible for the compliance with the Personal Data Law:
  - according to the information from the LinkedIn Websites, LinkedIn is responsible for the services of the website "linkedin.com" and this legal entity is the administrator of the domain name of the website "linkedin.com";
  - the "linkedin.com" website is hosted on technical platforms located in the United States which are owned by LinkedIn; and
  - under the Personal Data Law,[13] an operator of personal data is also defined as a legal entity which, among other things,

individual (https://www.linkedin.com/legal/user-agreement?trk=hb_ft_userag).

13 Art. 3, par. 2 of the Personal Data Law provides that an operator of personal data means a governmental body, municipal body, legal entity or individual that personally or jointly with other parties organizes and/or processes personal data and determines the purposes of personal data processing, the content of personal data to be processed and the actions (operations) involving personal data.

organizes and/or processes personal data in cooperation with other parties.

- the provisions of the Russian legislation are applicable to LinkedIn:
  - under the Information Protection Law,[14] the usage of information and telecom networks in Russia is subject to the requirements of Russian law;
  - under the Russian Civil Code,[15] the choice of law governing a contract may not deprive a consumer of the protection of their rights provided by the mandatory provisions of the law of the country of the consumer's place of residence if the other party to the contract (the professional party) in any way focuses its activities on the country of the consumer's place of residence; and
  - LinkedIn focused its activities on Russia because, in particular, (a) the LinkedIn Websites have a Russian version and provide for the placement of advertising in Russian, and (b) LinkedIn, being an entity engaged in business activities, understands that restricting access to the LinkedIn Websites in Russia will affect its interests.

As of the date of this client update, the LinkedIn Websites remain inaccessible in Russia.

This client update was originally issued on February 14, 2017.

---

[14] Art. 15, par. 1 of Federal Law No. 149-FZ on Information, Information Technologies and Protection of Information dated July 27, 2006 (the "Information Protection Law").

[15] Art. 1212, par. 1 of the Civil Code of the Russian Federation (Part 3) No. 146-FZ dated November 26, 2001 (the "Russian Civil Code").

Fines for Personal Data Violations in Russia Increase as of July 1, 2017

On January 27, 2017, Bill No. 683952-6 on Amendments to the Code of Administrative Offences of the Russian Federation[1] was adopted in the third reading by the State Duma of the Russian Federation ("Bill"). The Bill provides for tiering and a five to ten times increase of fines for violation of personal data laws for individuals, company officers and legal entities.[2] Although the increase of fines is still unsubstantial, it shows governmental attention to personal data protection in Russia and demonstrates the tendency towards tightening the rules in this sphere.

In particular, the Bill provides for the following fines:

- Processing of personal data inappropriate for the objectives of personal data collection will lead to the imposition of an administrative fine on company officers ranging from RUB 5,000 (approx. USD 83.00) to RUB 10,000 (approx. USD 167.00), and on legal entities ranging from RUB 30,000 (approx. USD 500.00) to RUB 50,000 (approx. USD 833.00);
- Processing of personal data without the consent of the subject of the personal data where such consent was required under the law[3]

---

1 Information on the Bill is *available at* http://asozd2.duma.gov.ru/main.nsf/%28Spravka%29?OpenAgent&RN=683952-6&02.

2 Pursuant to the current version of Article 13.11 of the Code of Administrative Offences of the Russian Federation (the "Code"), failure to comply with the procedure for collection, storage, use or dissemination of personal data set forth by the law may lead to the imposition of an administrative fine on company officers ranging from RUB 500 to RUB 1,000, and on legal entities ranging from RUB 5,000 to RUB 10,000.

3 *E.g.*, written consent for processing of personal data is required for cross-border transfer of personal data to a jurisdiction that does not provide for

or failure to comply with the requirements for the mandatory information to be included in a written personal data processing consent[4] will lead to the imposition of a fine on company officers ranging from RUB 10,000 (approx. USD 167.00) to RUB 20,000 (approx. USD 333.00), and on legal entities ranging from RUB 15,000 (approx. USD 250.00) to RUB 75,000 (approx. USD 1250.00);

- Failure by the personal data operator to publish its personal data processing policy or otherwise make it publicly available will lead to the imposition of an administrative fine on company officers ranging from RUB 3,000 (approx. USD 50.00) to RUB 6,000 (approx. USD 100.00), and on legal entities ranging from RUB 15,000 (approx. USD 250.00) to RUB 30,000 (approx. USD 500.00);
- Failure by the personal data operator to provide information to the personal data subject relating to the processing of his/her personal data[5] will lead to the imposition of an administrative fine on company officers ranging from RUB 4,000 (approx. USD 67.00) to RUB 6,000 (approx. USD 100.00), and on legal entities ranging from RUB 20,000 (approx. USD 333.00) to RUB 40,000 (approx. USD 667.00).
- Failure by the personal data operator to comply within the prescribed period with a request to update or block or delete personal data where such personal data are incomplete, not up to date or inaccurate, or were obtained on non-legal grounds, or are

---

adequate protection of rights of personal data subjects (Article 12 of Federal Law No. 152-FZ on Personal Data dated 27 July 2006) (the "Personal Data Law").

4 Such information is specified in Article 9 of the Personal Data Law.

5 A list of such information is provided in Article 14 of the Personal Data Law.

not appropriate for the specified objectives of the processing will lead to a fine on company officers ranging from RUB 4,000 (approx. USD 67.00) to RUB 10,000 (approx. USD 167.00), and on legal entities ranging from RUB 25,000 (approx. USD 471.00) to RUB 45,000 (approx. USD 750.00).

- Failure by the personal data operator that carries out non-automated processing of personal data to ensure security of any material media containing such personal data or to prevent unauthorised access thereto if this has resulted in unauthorised or accidental access to such personal data; the destruction, modification, blocking, copying, provision or dissemination of such personal data; or any other unauthorised acts in respect of such personal data will lead to the imposition of an administrative fine on company officers ranging from RUB 4,000 (approx. USD 67.00) to RUB 10,000 (approx. USD 167.00), and on legal entities ranging from RUB 25,000 (approx. USD 417.00) to RUB 50,000 (approx. USD 833.00);
- Failure by a governmental authority or municipal body to depersonalise personal data or to comply with the existing requirements or procedures for depersonalisation of personal data will lead to a warning or imposition of an administrative fine on officials ranging from RUB 3,000 (approx. USD 50.00) to RUB 6,000 (approx. USD 100.00).

After the Bill is approved by the Federation Council and signed by the Russian President, the new fines become effective as of July 1, 2017.

This client update was originally issued on February 1, 2017.

Contributors

LUKE DEMBOSKY

Luke Dembosky is a litigation partner based in the firm's Washington, D.C. office. He is Co-Chair of the firm's Cybersecurity & Data Privacy practice and a member of the White Collar & Regulatory Defense Group. His practice focuses on cybersecurity incident preparation and emergency response, related civil litigation and regulatory defense, as well as national security issues. Mr. Dembosky is a recognized leader in the industry by numerous publications, including the *National Law Journal*, *Cybersecurity Docket*, *The Legal 500 US* and *Chambers USA* 2018. Prior to joining the firm in 2016, Mr. Dembosky served as Deputy Assistant Attorney General for National Security in the National Security Division of the U.S. Department of Justice where he was responsible for overseeing the Department of Justice's first national security cyber portfolio. He previously served as Deputy Chief for Litigation in the Computer Crime and Intellectual Property Section, and before that as the Department of Justice's representative at the U.S. Embassy in Moscow.

JEREMY FEIGELSON

Jeremy Feigelson, a litigation partner, is Co-Chair of the firm's Cybersecurity & Data Privacy practice and is a member of the firm's Intellectual Property and Media Group. He frequently represents clients in litigation and government investigations that involve the Internet and new technologies. His practice includes litigation and counseling on cybersecurity, data privacy, trademark, false advertising, copyright, and defamation matters.

JEFFREY P. CUNARD

Jeffrey Cunard, managing partner of the Washington, D.C. office, leads the firm's corporate information technology and intellectual property practices, where he focuses on data protection, privacy, cybersecurity and Internet law matters. He has broad experience in transactions, including mergers and acquisitions, licenses, joint ventures and outsourcing arrangements. Mr. Cunard's practice also encompasses litigation at the intersection of copyright and technology.

DAVID A. O'NEIL

David A. O'Neil is a litigation partner and member of the firm's White Collar & Regulatory Defense Group. His practice focuses on white collar criminal defense, internal investigations, privacy and cybersecurity, congressional investigations, and AML/sanctions enforcement defense. Prior to joining the firm in 2015, Mr. O'Neil served for eight years in prominent positions within the Department of Justice, most recently in the Criminal Division where he was responsible for supervising more than 600 attorneys investigating and prosecuting the full range of federal crimes, including corporate malfeasance, cybercrime, fraud offenses and money laundering. Mr. O'Neil began his career as a federal prosecutor in the U.S. Attorney's Office for the Southern District of New York.

JIM PASTORE

Jim Pastore is a litigation partner and a member of the firm's Cybersecurity & Data Privacy practice and Intellectual Property Litigation Group. His practice focuses on privacy and cybersecurity issues. Prior to rejoining Debevoise in 2014, Mr. Pastore served for more than five years as an Assistant United States Attorney in the Southern District of New York. While he was with the Criminal Division of the U.S. Attorney's Office, Mr. Pastore spent most of his time as a prosecutor with the Complex Frauds Unit and Computer Hacking and Intellectual Property Section. From 2004 to 2009, Mr. Pastore was an associate at Debevoise focusing on IP litigation.

PAUL RODEL

Paul Rodel is a corporate partner and member of Debevoise's Capital Markets, Banking, Private Equity and Latin America Groups. He represents U.S, Latin American and European companies in the financial services, energy, banking and media industries in registered, private and offshore capital markets transactions. Mr. Rodel is frequently a speaker and author on securities regulation and corporate governance issues, including recently on the disclosure and reporting approaches taken by companies affected by cybersecurity events, multijurisdictional disclosure requirements with regard to environmental and climate change issues, the impact of proxy advisors on corporate governance, recent developments in insider trading, current trends in cross-tender offers, recent development in growth company initial public offerings, regulation of conflicts of interest in analyst research as well as key disclosure issues for banking organizations

JANE SHVETS

Jane Shvets is a partner in the London office of Debevoise & Plimpton. She advises clients on data protection and cybersecurity matters, as well as on white collar defense and internal investigations. Ms. Shvets has represented a variety of U.S. and foreign corporate clients, with a particular emphasis on Eastern Europe and Russia. Ms. Shvets is recommended as a leading lawyer in *The Legal 500 UK* (2017), and is named by *Global Investigations Review* amongst the most prominent women in the world advising on investigations today.

Acknowledgements

The authors would like to thank Debevoise associates Stephanie Cipolla, Christopher Ford, Azeezah Goodwin, and Joshua Shirley, as well as former associate Julia Shu, for their invaluable contributions to Breach Reading 3.0, including their research, drafting, and revising of the materials. A special thank you to Richard Fitch, Fred Loessel, Caroline O'Neill, and the rest of the production team for their work in pulling all of this together. We would also like to recognize the important contributions from Debevoise summer associates Michael Bloom, Thamanna Hussain, and Victoria Jimenez. We appreciate all the hard work.

Debevoise & Plimpton

919 Third Avenue
New York, NY 10022
+1 212 909 6000

801 Pennsylvania Avenue N.W.
Washington, D.C. 20004
+1 202 383 8000

65 Gresham Street
London
EC2V 7NQ
+44 20 7786 9000

4 place de l'Opéra
75002 Paris
+33 1 40 73 12 12

Taunustor 1 (TaunusTurm)
60310 Frankfurt am Main
+49 69 2097 5000

Business Center Mokhovaya
Ulitsa Vozdvizhenka, 4/7
Stroyeniye 2
Moscow, 125009
+7 495 956 3858

21/F AIA Central
1 Connaught Road Central
Hong Kong
+852 2160 9800

13/F, Tower 1
Jing'an Kerry Centre
1515 Nanjing Road West
Shanghai 200040
+86 21 5047 1800

Shin Marunouchi Bldg. 11F
1-5-1 Marunouchi, Chiyoda-ku
Tokyo 100-6511
+81 3 4570 6680

www.debevoise.com