Debevoise & Plimpton

Breach Reading

A Midyear Review of Cybersecurity & Data Privacy

2015

Debevoise & Plimpton

Breach Reading

A Midyear Review of Cybersecurity & Data Privacy

Contents

Contents (cont'd)

Introduction

By: Bruce E. Yannett

Cybersecurity is an issue confronting all companies – large and small, public and private. Hardly a day passes without headlines involving new data breaches, state-sponsored attacks, regulatory actions, or proposed legislation. It is essential that in-house counsel, executives, and directors understand the threats to their companies' data, how they can guard against attacks, how to respond to an attack, and the legal and policy implications of such attacks.

Although the cybersecurity threat is real and pervasive, the law governing this area is still being written today, by regulators, legislators, and courts. Best practices and legal obligations are changing almost as rapidly as the technologies and vectors of malicious attacks.

This brief guide, written by Debevoise's team of experts in the field of cybersecurity and data privacy, is intended to provide a snapshot of where things stand midway through 2015. We have surveyed recent developments in private litigation, regulatory action, sector-specific news, international law, and legislation to provide you with an overview of emerging issues, new guidance, and fundamentals – everything from the widely discussed NIST framework to the specific privacy concerns in moving data across borders.

Our goal is not to provide a comprehensive, in-depth introduction to the field of cybersecurity: there is plenty more to say about each of these topics, and each business has a unique cybersecurity profile both in terms of its defenses and the threats it faces. Rather, we are providing this compilation of original articles and recent client

updates to give you a single resource for recent events, emerging best practices, and a hint of what's to come in the next several months.

We hope you find it a useful resource, and we are available to discuss these or other issues you may be interested in.

Private Litigation

"I just hacked one billion passwords by guessing '12345.'"

Our first section deals with trends in private litigation stemming from data breaches. We provide an overview of the types of private litigation that can result from a data breach, from shareholder derivative suits to consumer class actions.

We focus in particular on class actions. The big news is that, after a virtually unbroken string of successes in defeating data breach class actions at the motion to dismiss stage, there have been two recent and potentially significant setbacks for companies defending themselves against plaintiffs' claims. The first came in a pair of decisions by the District Court in litigation stemming from the

Target data breach. The second was a more-recent Circuit-court ruling that revived class action claims against Neiman Marcus stemming from its breach.

In this section and throughout this book, we gather some of our most-relevant Client Updates, which Debevoise issues regularly throughout the year on a variety of topics including cybersecurity and data privacy.

The Second Wave:
After the Breach Response Come the Class Actions

When a company's systems are breached, the number of potentially affected customers, clients, or business partners can run into the tens of millions. And with such large numbers of potential victims comes the threat of class-action litigation.

Plaintiffs in these class-action cases – usually consumers, but sometimes employees or financial institutions – have faced a number of substantive and procedural hurdles. But some suits have gained traction, and even where plaintiffs do not obtain all of the relief they are seeking, companies may find themselves offering expensive settlements and incurring considerable legal costs litigating multiple actions in a number of different jurisdictions.

THEORIES OF LIABILITY

Consumers

Most post-breach class actions have been brought by the plaintiffs' bar on behalf of purported classes of consumers. These cases have advanced a broad range of theories of liability, from the common law to federal and state statutes.

Among the common law claims, the plaintiffs' bar has argued that the company breached an express contractual obligation to keep safe its customers' personally identifiable information. It has also been asserted that simply by being the custodian of sensitive personal information, the company made an implied promise to keep such information secure. The plaintiffs' bar has also claimed that companies were negligent in allowing a data breach. On this theory, a company owed a duty to take reasonable care in protecting

customer information and failed to fulfill this duty, as evidenced by the fact of the breach and/or by the company's purported failure to timely notify customers after the breach. Still other claims include bailment (*i.e.*, the company had a duty to safeguard and return the personal information they held for another), negligent hiring (with respect to employees responsible for the breach), and invasion of privacy.

A number of federal and state statutes offer potential causes of action to consumer data breach class action plaintiffs. Some of these statutes require notice after a breach occurs; currently, 47 states have their own versions of these notification laws, and Congress is considering a national version. Additionally, many states have consumer protection statutes that contain private rights of action used by post-breach plaintiffs. Federal statutes are less availing to consumer plaintiffs, as claims under these laws are more novel and, so far, less successful. (For example, the plaintiffs' bar has argued that companies in possession of consumers' personally identifiable information are "consumer reporting agencies" for purposes of the Fair Credit Reporting Act (FCRA), and are accordingly prohibited from furnishing consumer information except when specified by the statute. These claims have not met with much success.)

Other plaintiffs: shareholders, financial institutions, and employees
While most post-breach class actions have been filed on behalf of consumers, class action suits also have been brought on behalf of other purportedly aggrieved parties.

Suits have been filed on behalf of company **stockholders** as well. These claims fall into two general types. First, stockholders have written demand letters and brought complaints derivatively, on behalf of the company, seeking to hold directors and executives

liable for purported breaches of fiduciary duty. Second, shareholders have brought class actions under the securities laws, arguing that companies' disclosures or public statements relating to cybersecurity and the breach itself were inadequate. These suits further underscore that corporate directors and officers would do well to consider what steps a company's board is taking with respect to data security.

In the wake of the Sony Pictures hack, six class action suits were filed on behalf of current and former **employees** at that company. The complaints asserted claims under a variety of California data breach and business practices statutes, as well as common-law claims. These suits highlight that potential claimants may emerge from within a company as well as from outside.

The Target breach illustrates the potential for **business-to-business** class actions in the wake of a breach. A federal judge declined to grant Target's motion to dismiss claims brought by a class of credit-card issuers, who argued that Target owed them a common-law duty of care even in the absence of a direct contractual relationship between the retailer and the issuers of its customers' credit cards.

PLAINTIFFS' HURDLES: CLASS CERTIFICATION, PLEADING HARM

Standing: establishing harm

Some class claims have foundered on the basic principle that in order to bring a lawsuit, plaintiffs must be able to articulate how they have been harmed. Post-breach class action plaintiffs have had a difficult time convincing judges that exposure to a data breach constitutes the kind of injury that entitles them to their day in court.

Many plaintiffs run into resistance from courts skeptical of claims based on an increased risk of future harm. A 2013 Supreme Court decision, *Clapper v. Amnesty International*, makes it more difficult to advance claims premised on speculative or future harms, as opposed to actual and imminent injuries.

The difficulty of articulating specific injuries has resulted in many post-breach class actions ending at the motions to dismiss stage. For example, P.F. Chang's successfully argued that consumer plaintiffs had not pled a causal link between any monetary losses and payment card information that was illicitly accessed after a data breach at the restaurant chain. The Target breach offers an example of when plaintiffs have overcome this hurdle. In that case, a federal district court judge held that consumer plaintiffs had alleged sufficiently specific harms including unlawful charges, blocked access to bank accounts, inability to pay other bills, and late-payment charges. More recently, as discussed in a Client Update later in this book, the Seventh Circuit revived a class action against Neiman Marcus stemming from a breach it suffered, reversing the district court's grant of a motion to dismiss and holding that the allegations of harm were sufficient – the first federal appellate court to so rule.

Class certification

Other post-breach class actions have faced another stumbling block: courts often refuse to certify a proposed class, *i.e.*, to let the range of proposed similarly aggrieved parties aggregate their claims and move forward with litigation.

In the data breach context, it can be difficult for a group of apparently similarly situated people to make the required showing that the factual and legal issues in a proposed lawsuit are applicable to all of them.

One example: After credit and debit card information was potentially compromised at Hannaford, a supermarket chain, a group of consumer plaintiffs moved to certify a class. Claimed damages included fees for new cards and money spent on identity theft insurance. A federal judge held that there was insufficient evidence that particular cardholders actually suffered fraudulent charges, and that those who did may have responded differently and incurred different kinds of costs. Without expert testimony demonstrating the feasibility of calculating damages on a class-wide basis, the court declined to certify the class.

SETTLEMENTS

Sometimes, companies choose to conclude post-breach class actions by settlement. These settlements have included financial payments; some have also included companies agreeing to implement new security policies.

Target's consumer class action litigation culminated in a settlement that saw the retailer agree to pay $10 million and put in place a number of policy changes. These included the appointment of a chief information security officer, developing a written information security program, and educating certain employees with respect to safeguarding consumer information.

Other settlements have featured sliding scales for payouts that may fluctuate based on the final number of eligible claims. In 2011, after a breach at their online brokerage, the company TD Ameritrade agreed to set aside as little as $2.5 million or as much as $6.5 million for a class of plaintiffs with identity-theft related claims after a breach at the online brokerage.

CONCLUSION

Post-breach class actions are becoming as inevitable as data breaches themselves, particularly for companies with large consumer-facing operations. Challenges to the commonality of a proposed class's factual and legal questions, as well as opposition on the grounds that plaintiffs have failed to plead a link between a breach and any specific harm, are common themes of successful post-breach class action defenses. While significant hurdles stand in the way of data breach class action plaintiffs, the specter of defending multiple suits across the country – and the willingness of some defendants to settle them at significant cost – underscores that this is a risk corporate counsel should take seriously.

Post-breach class action plaintiffs have had a difficult time convincing judges that exposure to a data breach constitutes the kind of injury that entitles them to their day in court.

Client Update:

Data Breach Plaintiffs' Suit Reinstated; Court Holds Affected Customers Have Standing

A new decision from the Seventh Circuit Court of Appeals holds that consumers of a hacked retailer had standing to sue on the basis of the costs they incurred in responding to the breach, even if their accounts had not suffered any fraudulent charges. The Court held that even consumers that had not experienced actual identity theft had standing to sue, given the costs allegedly associated with "sorting things out" in the wake of a data breach.

The Seventh Circuit's ruling bucks a longtime trend of post-data breach consumer class actions failing at the pleading stage in the wake of the Supreme Court's 2013 decision in *Clapper v. Amnesty International*. *Clapper* held, in the context of allegations of unlawful electronic surveillance, that an imminent risk of concrete injury is required for a plaintiff to have standing to sue in federal court. Many district courts have relied on *Clapper* to grant motions to dismiss data breach class actions, holding that the mere theft of information does not establish an imminent risk of concrete injury.

THE DECISION

The new decision in *Remijas v. Neiman Marcus Group, LLC* departs from that trend, reversing the decision of the district court to toss out the suit based on *Clapper*. Neiman Marcus suffered a data breach in 2013 that potentially exposed up to 350,000 credit cards, but according to the company, only 9,200 consumers actually suffered fraudulent transactions. Neiman Marcus paid for a year of identity theft monitoring for all 350,000 accounts. Plaintiffs in *Neiman Marcus* sued on a number of theories, arguing that they had standing

because of the lost time and money spent protecting against future identity theft.

The district court held that the plaintiffs lacked standing under *Clapper* because the harm was inchoate. The Seventh Circuit held that this interpretation of *Clapper* was too broad and did not appreciate the likelihood of future harm – "the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit card fraud in order to give the class standing."

IMPACT AND ANALYSIS

The *Neiman Marcus* analysis, if adopted by other courts, could give consumers standing in data breach cases because of the costs associated with protecting against identity theft and fraud. As the Seventh Circuit noted: "the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." In light of that reasoning, the Court held *Clapper's* requirement of imminent future injury satisfied.

Another significant aspect of the *Neiman Marcus* decision relates to the oft-asserted defense, in the wake of data breaches, that affected consumers' information could have been obtained from any number of hacked companies. Neiman Marcus noted the breadth of the Target hack, and asserted that Plaintiffs could not show that the breach at Neiman Marcus was the source of their problems. The Seventh Circuit held that this showing was not required: the fact that other companies might have exposed Plaintiffs' information was for defendants to prove, not for plaintiffs to allege.

Although the *Neiman Marcus* decision generally provides a boost to consumer suits, it is worth remembering that it deals only with whether plaintiffs can survive a motion to dismiss. The Court's

opinion repeatedly referenced the standard that requires courts to credit plaintiffs' allegations at this stage of the litigation, and noted all that is required to establish standing is a non-speculative assertion of injury.

Whether *Neiman Marcus* portends a paradigm shift remains to be seen. The new decision is particularly significant in light of the relatively recent decisions in the class action litigation stemming from Target's data breach. Two class actions against Target – one by consumers and one by financial institutions – survived motions to dismiss in December 2014. There, as in *Neiman Marcus*, the court found plaintiffs had standing given allegations of injury based on fraudulent charges and the time and costs involved in dealing with breach-related issues. Target ultimately settled the consumers' claims for $10 million. The financial institution class action remains pending after a proposed $19 million settlement fell apart when not enough banks signed on. Given that a circuit court has now adopted reasoning similar to the *Target* class action cases in refusing to dismiss class action claims stemming from a data breach, there is little doubt that the plaintiffs' class action bar will continue to bring post-breach damage cases.

This client update was originally issued on July 28, 2015.

Client Update:

Proposed Target Settlement Provides Roadmap for Future Consumer Settlements in Large-Scale Data Breach Cases

On March 19, 2015, United States District Judge Paul Magnuson of the District of Minnesota gave preliminary approval to a proposed settlement in the multi-district consumer litigation brought against Target Corporation in the wake of its 2013 data breach that exposed the credit card and personal information of up to 110 million customers. If given final approval, the settlement will resolve one of the largest ever consumer class actions stemming from a breach of payment-card security, and therefore could provide a roadmap for what future large-scale data breach settlements may look like.

ESTABLISHMENT OF A FUND TO PAY CLASS MEMBERS

Target has agreed to pay $10 million into an interest-bearing escrow account. Consumers who used credit or debit cards at Target stores between November 27, 2013 and December 18, 2013 will be eligible to receive up to $10,000 each by submitting proof of costs associated with identity theft, unauthorized charges and higher interest rates that resulted from unauthorized activity on their credit accounts. Class members may also submit claims for time spent addressing these issues, although recovery is limited to $10 an hour, with a cap of two hours. Although "lost time" is often proffered by plaintiffs as a basis for alleging damages stemming from a breach, courts generally have rejected this theory of damages. See, *e.g.*, *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 671 F. Supp. 2d 198, 201 (D. Me. 2009) (certifying questions to the Maine Supreme Judicial Court as answered in *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492, 496-98 (Me. 2010)). The fund will prioritize payments to consumers who can document their losses, while other class members will receive a share of any remaining

funds. The Court will distribute any remaining funds, though the details of those disbursements are left undefined by the settlement.

Given the magnitude of the breach, the $10 million figure is likely lower than Target would have faced with a ruling on the merits, which may be indicative of the difficulties consumers face in proving cognizable damages in data breach cases. In fact, Judge Magnuson's opinion denying Target's motion to dismiss cautioned that the plaintiffs might have trouble establishing damages at later stages in the litigation. See *In re Target Corporation Customer Data Security Breach Litigation*, District of Minnesota, 14-md-02522 (dkt. no. 281.)

NON-MONETARY MEASURES TO BOLSTER SECURITY

The settlement also requires Target to take a series of non-monetary steps designed to better safeguard customer data, including:

- Hiring a chief information security officer to coordinate and take responsibility for its information security program entrusted with the protection of consumers' personal information;
- Maintaining a written information security program that identifies internal and external risks to the security of consumers' personal information and mandates periodic review of the sufficiency of safeguards to control such risks; and
- Implementing a program to educate and train relevant employees about the security of consumers' personal information.

These unique terms highlight the obligations increasingly imposed on organizations to maintain adequate data security policies to safeguard consumer data.

A final approval hearing on the proposed settlement has been scheduled for November 10, 2015.

The settlement does not resolve a pending class-action lawsuit by financial institutions against Target that seeks compensation for breach-related expenses such as reissuing affected payment cards and covering the cost of fraudulent charges. (Dkt. no. 163). Significantly, in December 2014, Judge Magnuson denied Target's motion to dismiss, holding that the financial institutions adequately had pled the existence of a "special relationship" between Target and the financial institutions such that Target had a duty to adequately protect customer credit and debit card data. The Court also refused to dismiss the banks' negligence claims against Target for its alleged failure to provide a sufficient level of security that could have prevented the breaches. (Dkt. no. 261).

Target also continues to deal with a number of state and federal investigations into the breach.

The *Target* consumer class-action settlement is a significant development for breach-related litigation, but the legal fallout from Target's data breach is not yet over, and we can expect that courts and regulators alike may increasingly seek to hold companies liable when they suffer data breaches if the court concludes that the company failed to take adequate measures to safeguard sensitive customer data.

This client update was originally issued on April 1, 2015.

Industry Watch

" A hacker broke into our computer system and, in a random act of kindness, organized all of our files. "

Cybersecurity is a top challenge facing all businesses in 2015. In this section, we discuss some of the particular concerns, and potential action items, for the healthcare and private equity sectors.

In each of these sectors, cybersecurity is reshaping old concerns and creating new threats and challenges. Although sensitive data like health information and credit card numbers were always considered

valuable, new technologies – and new actors, like hacktivists and nation-states – have changed the landscape for many different industry players. For private equity firms, which may have portfolio companies across several higher-risk sectors, attention to cybersecurity matters can play a significant role in protecting their investments.

In these articles, we present a basic picture of what each industry has recently experienced and what trends are likely to dominate the conversation for the rest of the year.

The ~~Doctor~~ Hacker Is In:

Cybersecurity Threats Facing Healthcare Companies

OVERVIEW

Healthcare companies hold some of the data assets that are most enticing to hackers: patient medical records that often contain a full range of personally identifiable information and, unlike a credit card number, cannot be cancelled and rendered void. From thieves looking to cash in on a black market that prizes medical data, to agents of foreign governments seeking targets' identifying information via their health records, malicious cyber actors have trained their sights on the holders of those records.

These breaches signal health insurers' particular exposure to cybercrime

These breaches signal health insurers' particular exposure to cybercrime and illustrate the legal consequences of the cybersecurity threat to a highly regulated industry with national reach. Insurers are not alone, however, as the FDA has recently issued guidance stating that both manufacturers and health care providers must be aware of the cybersecurity risks inherent in networked medical devices and online records, potentially a first step from the agency towards regulating Internet-enabled healthcare.

THE ANTHEM AND PREMERA BLUE CROSS BREACHES: BEGINNING OF A TREND?

In just the first several weeks of 2015, two of the country's largest health insurers reported significant breaches. The attack on Anthem, the second-largest U.S. health insurer, affected as many as 80 million people. While the impact was broad, the damage was not as severe as it could have been: the company reported that hackers were unable to obtain customers' medical information, instead

carting away information such as names, dates of birth, addresses, and Social Security numbers.

Around the same time, Premera Blue Cross reported that it, too, experienced unauthorized access to its systems. That breach affected fewer individuals but, in addition to the kinds of personal information exposed in the Anthem attack, Premera reported that hackers may have accessed customers' clinical and financial records.

WHO WANTS INSURERS' DATA, AND WHY

The rich stores of personal information held by health insurers hold obvious appeal to financially motivated cybercriminals. In addition to holding large amounts of personally identifiable information in one place, health insurers hold medical records that are considered to be far more valuable than other types of consumer information. Experts estimate that a stolen medical record can be sold on the black market for about $50 per record, many times more than other types of consumer information.

Medical records are more valuable than other consumer data in part because hackers can use information collected from insurers for a variety of different purposes. Stolen medical information can be used to buy medical equipment or drugs, or to file false claims with healthcare companies. The large amount of information contained in one individual's single medical file facilitates complex identity theft operations.

Recent reports suggest that a group of Chinese hackers, with possible government connections, were behind both the Anthem and Premera attacks as well as the recent incursion into the systems of the U.S. Office of Personnel Management, in which over 22 million records were compromised. That points to the foreign

intelligence value of the stolen data. Among other things, government officials and corporate executives who otherwise operate discreetly generally must use their real names and other identifying information in their health records.

THE RISKS OF INTERCONNECTEDNESS

In addition to holding particularly sensitive information, insurers are often structured in a way that facilitates large-scale attacks from a single point of entry. Because various insurers are often party to "business associates" agreements designed to create a national claims-processing network, a breach at one insurer may expose information held across a network. The 2015 Anthem breach is a case in point: as noted above, that incident exposed around 80 million people's records – but Anthem itself has just under 40 million members. Reports indicate that up to 1.1 million CareFirst members may also have been affected by the Anthem breach because their claims information is stored across the Blue Cross and Blue Shield healthcare networks.

LEGAL IMPLICATIONS

Both the Anthem and Premera breaches were followed by a slew of class action suits. Complaints in these suits alleged, among other things, that Premera waited unacceptably long before notifying customers of the breach, and that Anthem failed to put appropriate safeguards in place after past cybersecurity incidents put the company on notice of future risks.

In addition to these sorts of claims, health insurers must consider data breaches in the context of the Health Insurance Portability and Accountability Act (HIPAA). In 2013, changes to the HIPAA Privacy and Security Rules made any organization that handles patient information under a "business associate" agreement with a

HIPAA "covered entity" just as liable for breaches as the covered entity itself. In the context of a breach like the one at Anthem that affected organizations across the BlueCard reciprocal claims payment network, rules like these cast a broad net of potential legal liability – even when a breach doesn't occur in an insurer's or another healthcare organization's own systems.

INVESTING IN SECURITY IS EXPENSIVE, BUT BREACHES COST MORE

The Anthem and Premera breaches came with significant price tags for the two insurers, as well as a number of business partners. In addition to incurring expenses pertaining to breach notification, Anthem also arranged for affected consumers to receive free identity protection services for two years. Reports estimate that Anthem's data breach will cost the company over $100 million. These financial costs are compounded by the risk of losing customers in the wake of a breach. A study conducted by the Ponemon Institute determined that the pharmaceuticals, communications and health care industries lose customers due to breaches at the highest rate of any industry.

The Anthem and Premera experiences shed light on what health insurers can do to mitigate risks and reduce future costs. Companies may wish to refer to an emerging set of best practices that includes things like encrypting stored data, increasing investments in systems monitoring capabilities, and educating employees to avoid opening the door to intruders.

Health insurers may also want to consider the best way of beginning or continuing a dialogue with their customers and business partners about potential security risks. Consumer surveys suggest that people do not typically check their medical records, often because they don't know how. Healthcare companies may want to consider how

to best educate their customers and encourage cooperation in securing their private information.

CONCLUSION

Experts estimate that a stolen medical record can be sold on the black market for about $50 per record, five times as much as other types of consumer information.

Health insurers hold a particularly valuable store of private information, and are accordingly a compelling target for hackers with a range of interests and capabilities. Additionally, the interconnectedness of insurers, providers, and other healthcare organizations means a breach at one site can reach far and wide – spreading potential damage as well as potential legal liability. Given these peculiar risks, health insurers should consider where they stand with the emerging best practices of cybersecurity preparation and response.

Cybersecurity and Private Equity:
Securing the Firm and the Portfolio

The threats facing private equity firms[1] and their portfolio companies run the gamut from insider attacks by employees to data theft by organized criminal enterprises. The costs of these attacks can include not only the short-term expenditures associated with the breach response, but also long-term reputational harm for the firm or, if portfolio companies are breached, the firm's investments. Responding in part to these complex threats, regulators have signaled that they intend to increase their scrutiny of the cybersecurity posture of registered investment advisers.

Against this backdrop, private equity firms should consider taking a risk-based approach that addresses cybersecurity risks of (1) the firm, where sensitive data such as material non-public information and the personally identifying information of employees and limited partners (LPs) may be stored, and (2) its portfolio companies at each stage of the private equity lifecycle, *i.e.*, pre-acquisition, when due diligence of a target could include a review of its cybersecurity posture, and post-acquisition when attention to ongoing cybersecurity preparedness of portfolio companies can help protect the firm's investments by preventing data breaches or mitigating harm should a data breach occur.

In this arena, one size certainly does not fit all. Cybersecurity protections should be tailored to the size of the firm and its assets

[1] In this article where we refer to a private equity "firm," for ease of reference we refer not only to the investment adviser and its affiliated management entities but also to the funds and separate accounts sponsored and managed by the firm.

under management, the size and nature of its portfolio companies' businesses, and the types and volume of data that it and they maintain. Still, private equity firms of all types and sizes can look to a common set of basic metrics and behaviors that will help them assess cyber threats and manage the business and legal risks that cybercrime poses to the firm and its investments.

THE FIRM

Paying attention to cybersecurity at the private equity firm itself isn't just good business; increasingly, it is becoming a regulatory expectation. The SEC's Office of Compliance Inspections and Examinations (OCIE) has labeled cybersecurity compliance a matter of crucial importance that will be subject to increased scrutiny in the coming years.[2] In 2014 OCIE examined a significant percentage of all the newly registered private fund advisers, and included among its examination priorities a review of those advisers' cybersecurity compliance and controls. Recently OCIE publicly reiterated that cybersecurity compliance and controls remain examination priorities in 2015. Expanded regulation requires the private equity industry to continue to focus on changing cybersecurity best practices.

Well-recognized benchmarking standards, such as the Cybersecurity Framework promulgated by the National Institute of Standards and technology (NIST), the SANS-20 Critical Security Controls, or ISO 27001, can help firms begin to understand their cybersecurity

[2] As we addressed in the client update "SEC Issues Cybersecurity Guidance for Registered Investment Advisors and Funds" (included in this publication), the SEC has issued guidance suggesting that registered investment advisers and funds need to manage cybersecurity risk, including preparing to respond to a cyberattack – or risk running afoul of the U.S. securities laws.

exposure, and how to manage it.[3] Regardless of which standard a firm chooses to adopt, a cybersecurity program begins with gathering and organizing detailed information on the firm's assets and architecture. This means documenting what assets the firm has (*i.e.*, the assets that might be the target of hackers) and where those assets are kept (*i.e.*, the firm's architecture, such as servers, desktops and mobile devices). This task is easier said than done. We have found in our work for companies, large and small, that the process of mapping assets and architecture is likely to uncover a number of surprises and, potentially, weaknesses.

A private equity firm's assets can include sensitive personal and financial information of the founders and other employees of the firm; data concerning the sovereign wealth funds, financial institutions, foundations and other LPs of the funds managed by the firm, such as data gathered to satisfy KYC / AML requirements; material non-public information about the portfolio companies themselves and the firm's plans (exit and otherwise) with respect to those portfolio companies; and confidential information about the firm's own strategy and potential fund investments.

Knowing a firm's assets is only half the battle, however. Understanding the firm's architecture is equally important. This means knowing, for example, exactly where the firm stores its sensitive data (*e.g.*, internationally, off-site, with a third-party cloud provider or using an application services provider); its level of protection; whether the network is "segmented" so that an intruder who gets in the front door does not have the run of the whole house; and whether stale files are periodically purged.

---

[3] The fourth section of this publication covers in more detail two methods for assessing a company's cybersecurity posture.

Once a firm has analyzed its assets and architecture, the next steps are (1) developing a plan to protect those assets by establishing control measures and (2) determining in advance how best to respond to a breach incident, should one occur. Controls come in many varieties and can be specifically tailored to fit the specific needs of a firm. One method for maintaining the technological edge is by conducting third-party penetration tests (a/k/a "hire-a-hacker") to identify holes in security. Such tests can also provide an opportunity to test the adequacy of incident management procedures and incident management teams.

Ideally, responsibilities for incident response are well-defined by senior management of the firm and delineate clear reporting requirements. Answering the following questions can help develop a well-functioning and robust incident response plan:

- What types of business continuity plans are in place in the event of a cyberattack?
- Are reporting positions consolidated so that information about breaches can effectively be passed up the chain of command?
- How often does the firm conduct training and how effective is that training?
- What kinds of protections does the firm contractually require third-party vendors to employ to deter cyberattacks?
- What type of insurance coverage for cybersecurity-related events has the firm purchased?

PORTFOLIO COMPANIES: PRE-ACQUISTION

Cybersecurity also has begun to emerge as an issue to be explored during the due diligence process when a private equity firm is evaluating a potential portfolio investment. Here, again, one size certainly does not fit all. As an initial matter, firms can consider

whether the target operates in a sector with heightened cyber risk. Targets whose primary business is their intellectual property (*e.g.*, most technology companies), or that operate in certain sectors, may face greater cyber risk than, for instance, an industrial plant. But some level of cyber risk exists in every type of business. For example, a report released in December 2014 disclosed that hackers who infiltrated a German steel mill successfully caused massive damage to a blast furnace by manipulating the computers that controlled it.

Depending on the target's risk profile, a firm may do well to investigate and assess pre-acquisition the adequacy of the protections in place at the target. The questions that a firm may want to ask include:

- Is the target's value something that can be easily damaged by cyberattack?
- Can you tell whether that value has been compromised or will you be able to tell in the future?
- What types of monitoring mechanisms are in place to protect assets?
- Has the target recently been subject to expanded regulatory oversight or new rules and standards requiring capital investment or changes in the business model?
- Are you willing to pay the costs of establishing systems to protect your acquisition?

Firms also should be aware of any upcoming regulatory changes in the target's sector that could result in post-closing costs to remain compliant with new technology regulations. For instance, retailers who process credit card transactions from the major card brands must comply with a series of regulations known as the Payment

Card Industry Data Security Standard (PCI-DSS). As that standard evolves, so, too, will the steps that retailers must take to remain compliant. Beginning October 1, 2015, retailers who fail to implement "EMV" technology – which uses a chip embedded within the credit card to generate a unique value for each transaction during which the card is swiped through a cash register – will be responsible for all fraudulent charges made by swiping credit cards on their point-of-sale terminals. Firms thinking about acquiring a retailer may do well to explore whether the retailer has taken steps to comply with these regulations or, if it has not, what the remediation costs may entail.

PORTFOLIO COMPANIES: POST-ACQUISITION

Attention to cybersecurity should not end once the deal closes. Actively monitoring portfolio companies' cybersecurity programs can help protect the firm's investments, and regulators increasingly expect it. By way of example, in June 2014, SEC Commissioner Luis Aguilar cautioned that "Boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril."

Among the questions that private equity firm personnel who serve on the board of a portfolio company might want to ask are the following:

- When was the board last briefed on cybersecurity? Is there a regular schedule for such briefings?
- Who on the board "owns" cybersecurity risk management? For larger boards, is the audit committee or another committee charged with oversight?
- Have there been any prior data security incidents? If so, how were they handled and what was done to learn from them?

- Does the company have an incident response team and plan? If so, does it involve external as well as internal stakeholders? When was the last time it was tested?

The post-closing phase is also a good time to put in place remediation plans for cybersecurity weaknesses that were identified during due diligence, but which were not considered significant enough to derail the deal.

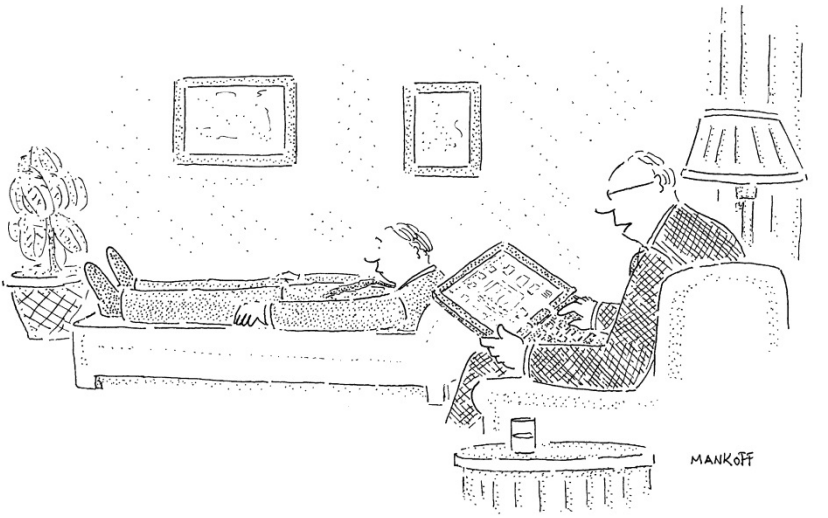
These are not just boxes to be ticked to satisfy regulators. Even state of the art cybersecurity programs cannot assure complete protection from the ongoing threat posed by ever more sophisticated cybercriminals, outside and inside an organization. Firms and companies that fail to focus based on these threats do so at their peril. As demonstrated by a series of well-publicized breaches, a failure in cybersecurity can have catastrophic business effects, resulting in reputational damages and substantial out-of-pocket losses.

CONCLUSION

Private equity firms of all types and sizes can look to a common set of basic metrics and behaviors that will help them assess cyber threats and manage business and legal risks.

Given the complexity of their operations, private equity firms face cybersecurity risks on a number of levels. A well-planned and robust cybersecurity program can help private equity firms avoid reputational damage, mitigate onboarding risk through acquisition, and secure their investments for successful exits.

Regulatory Actions



"Oops! I just deleted all your files. Can you repeat everything you've ever told me?"

Regulators have remained active in the cybersecurity space, with several state and federal entities jockeying for position as the prime mover in this space. We begin with an overview of enforcement priorities and actions. All eyes are on an important case pending before the Third Circuit in which Wyndham hotels is challenging the very basis upon which the Federal Trade Commission has brought some four dozen cybersecurity enforcement actions.

We also review in detail an important and, arguably, unprecedented case that the Federal Communications Commission brought against AT&T for allegedly failing to adequately safeguard the personal data

of nearly 280,000 customers at call centers in Mexico, Colombia and the Philippines. The case, which resulted in a $25 million settlement, signals the entry of yet another regulator into the cybersecurity arena.

We close with a selection of some of our Client Updates covering cybersecurity developments at the Securities Exchange Commission and the New York Department of Financial Services.

Regulation on the Rise:
Cybersecurity Enforcement Actions

INTRODUCTION

Cybersecurity enforcement actions remain on the rise. Continuing a trend seen in 2014, major regulators such as the Federal Trade Commission ("FTC"), the Securities and Exchange Commission ("SEC"), and the Department of Health and Human Services' ("HHS") Office of Civil Rights ("OCR") have been cracking down on companies for failing to prevent data breaches or otherwise to adequately secure consumers' personal information. This year the focus has been on companies that fail to use "readily available" security measures to protect sensitive data or who fail to regularly assess their security measures. Within its ambit, the Federal Communications Commission ("FCC") has pursued cybersecurity issues involving telecommunications companies.

ONGOING FTC ACTIONS IN 2015

The hottest issue in regulation remains whether the FTC even has the legal authority to make cases in this area. The FTC Act basically puts just two bullets in the Commission's legal arsenal, but what big bullets they are: under the statute, "unfair" and "deceptive" business practices are illegal. The FTC pursues companies in cybersecurity case on the theory that substantively inadequate cybersecurity is an unfair business practice, while security measures that are inconsistent with a company's public disclosures are deceptive. Two targets of FTC enforcement continue to push the view that the FTC has no authority to bring such cases. Some clarity should come later this year, or perhaps next.

The FTC continues to pursue its case in federal court against Wyndham for alleged security failures that resulted in three data

breaches at Wyndham hotels. Wyndham allegedly had taken insufficient measures to protect customer security. Wyndham has argued vigorously that the FTC cannot enforce cybersecurity standards that it hasn't formally promulgated. The FTC responded that the "soft guidance" available from its many individual enforcement cases suffices. The case was argued to the Third Circuit Court of Appeals in March. Whatever the outcome in the Wyndham case, companies are definitely now on notice that the FTC considers its enforcement actions to be precedent worth studying.

An FTC action against medical reporting company LabMD, Inc. is also ongoing. The complaint, originally filed in 2013, highlights the company's alleged failure to use "readily available measures" to prevent consumer billing information from being made publicly accessible, via an unauthorized file-sharing application that found its way onto the company network. LabMD has persistently challenged the FTC's legal authority, but the federal courts have declined to consider the challenge on its merits until the FTC resolves its administrative case. Trial proceedings before an administrative law judge appear to be nearing an end, amidst charges that the FTC case may be based in part on evidence fabricated by a disgruntled third party.

INCREASES IN FCC ENFORCEMENT ACTIVITY

Following the appointment of a new Enforcement Bureau Chief in early 2014, the FCC has exercised its enforcement power in data security cases involving telecommunications companies. The Commission's first cybersecurity enforcement action, filed in October 2014, levied fines of $10 million on telecommunications companies TerraCom Inc. and YourTel America Inc. The focus in these cases was on the companies' storage of unencrypted consumer

information on unprotected Internet servers, leaving it accessible to anyone in the world with a search engine. The FCC also highlighted the fact that the companies failed to employ "basic and readily available technologies" in order to secure the consumer information.

In April 2015, the FCC entered into a consent decree with AT&T Services, Inc. to resolve an investigation into three data breaches which took place at the company's foreign call centers, which we discuss in more detail in the next article in this section.

Separately, the FCC's Enforcement Bureau Chief has suggested that the FCC may be more assertive in exercising its enforcement authority going forward. Historically, many FCC investigations have ended in a settlement, where the agency and the enforcement target enter a consent decree, in which liability is not admitted. In the future, the FCC may insist that, in some circumstances, companies admit liability as a condition of resolving a matter.

HHS ENFORCING NEW PENALTIES UNDER HIPAA SECURITY RULE

The U.S. Department of Health & Human Services' Office for Civil Rights resolved a number of cases in 2014 under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)'s privacy and security rules, which apply to companies that have access to consumer's sensitive health data. The HIPAA Security Rule outlines the national security standards for companies that store sensitive healthcare information electronically. December 2014 marked the first time that OCR has enforced a penalty for using unpatched or outdated software, which is not specifically addressed in the HIPAA Security Rule. In December of 2014, Anchorage Community Mental Health Services (ACMHS) agreed to pay $150,000 and adopt a new security program as part of a settlement for violating the Security Rule. The OCR investigation

found that ACMHS had adopted security measures but failed to properly follow them or to "address and protect against basic risks [by] regularly updating their IT resources with available fixes." Additionally, ACMHS was running outdated software, which (according to OCR) contributed to its security deficiencies and put the personal health information of nearly 3,000 consumers at risk.

STATE AGS CONTINUE TO BE ACTIVE

A number of cybersecurity enforcement actions by state attorneys general were initiated in 2014, which saw a large uptick in collaborative, multistate investigations. This trend has continued into 2015, as several multistate actions have been launched or resolved in the past few months. In January, Zappos, Inc. agreed to pay $106,000 to the attorneys general of nine states as part of a settlement agreement related to a breach that occurred in 2012. In addition to the payment, Zappos must provide the attorneys general with its current security policy and copies of reports demonstrating compliance with the Payment Card Industry Data Security Standard for two years, and must have a third party audit its security practices regarding consumers' personal information.

In February of this year, the attorneys general of nineteen states launched a multistate investigation into JP Morgan Chase's security practices for sensitive consumer data in the wake of a data breach that occurred last year that led to the exposure of contact information for 76 million households and 7 million small businesses. The attorneys general involved in the case have now requested a "complete timeline of events leading up to the discovery of the breach" in addition to any reports that were compiled after the breach was discovered. The investigation is expected to focus on allegations that a more timely upgrade of certain systems to require two passwords for access might have prevented the breach.

CONCLUSION

Whatever the outcome in the Wyndham case, companies are definitely now on notice that the FTC considers its enforcement actions to be precedent worth studying.

It's clear that data security issues will remain a primary focus for government agencies. More regulators and self-regulatory groups may well join the fray in the near future – the SEC and FINRA both released cybersecurity reports in February, signaling their increased attention to security issues. Other agencies, including the Treasury Department, the New York Department of Financial Services and the Financial Stability Oversight Council (FSOC), have emphasized cybersecurity in recent speeches and annual reports, with DFS adding cyber to the list of topics covered by its regular exams of banks and insurers. As the body of regulatory enforcement actions grows, companies are given more and more signposts as to what sort of cybersecurity measures the government sees as legally required.

FCC Settles With AT&T Over Data Breach:

Advises Other Companies to Look to Settlement as Guidance

On April 8, 2015, the Federal Communications Commission ("FCC") announced a $25 million settlement with AT&T Services Inc. to resolve claims that the phone carrier failed to adequately safeguard the personal data of nearly 280,000 customers at call centers in Mexico, Colombia and the Philippines. The settlement is the agency's largest privacy and data security enforcement action to date and comes with an express directive for other companies to "look to this agreement as guidance" and "zealously guard" their customers' personal information.

The data breach resulted when employees at the call centers, operated by vendors of AT&T, accessed records belonging to roughly 280,000 customers based in the United States without authorization. Customer information – including names, full or partial social security numbers and other data – was then provided by the call center employees to third-parties who allegedly traffic stolen or secondary market phones. The third parties used the illegally obtained information to submit requests for codes in order to unlock the phones through AT&T's website.

Acting under its authority provided by the Communications Act of 1934, as amended by the Telecommunications Act of 1996, the FCC found that AT&T violated Section 222(a) of the Act, which requires telecommunications carriers to take every reasonable precaution to protect customer data, as well as Section 201(b), which makes it illegal for a carrier to employ "unjust or unreasonable" data security practices.

Although data security breaches have more traditionally been the focus of the Federal Trade Commission ("FTC"), this settlement demonstrates that the FCC has become more active, in part due to a rise in the number of mobile devices operating on FCC-regulated airwaves used by consumers to store personal information. Under the Act, the FCC may bring enforcement actions against telecommunication carriers, broadband providers and potentially other companies with a stake in mobile data security.

The $25 million fine levied against AT&T "ups the ante" for data breach cases investigated by the FCC and sends a strong message to companies that they must take steps to prevent data breaches if at all possible – not just from outside hackers, but from inside threats and third party vendors as well. The five previous enforcement actions taken by the FCC were valued at a total of only $50 million, the largest having been $10 million against TerraCom, Inc. and YourTel America, Inc. for failing to provide reasonable protection for consumers personal information.

The settlement also requires AT&T to enhance its protection of consumer information through a strict compliance program, including:

- Appointing a senior compliance manager who is a certified privacy professional;
- Conducting a privacy risk assessment;
- Implementing an information security program;
- Preparing an appropriate compliance manual;
- Regularly training employees on the company's privacy policies and the applicable privacy legal authorities; and
- Filing regular compliance reports with the FCC.

AT&T also agreed to notify all customers whose accounts were improperly accessed and to pay for credit monitoring services for customers affected by the breaches in Colombia and the Philippines. These actions are in addition to steps AT&T had previously taken following an internal investigation which brought the breaches to light, highlighting the importance of conducting independent internal investigations as soon as any red flags arise. Those steps included notifying customers whose information had been accessed in Mexico, terminating its relationship with the Mexican call center, investigating the other call centers, developing new monitoring procedures to identify suspicious account access and changing its unlock policy.

The $25 million fine sends a strong message to companies that they must take steps to prevent data breaches if at all possible – not just from outside hackers, but from inside threats and third party vendors as well.

As highlighted by the FCC, these steps provide guidance to all companies – even those not falling under the scope of the FCC's authority – to build a comprehensive information security program. The agreement can be looked at as a set of best practices for building a strict compliance program. Given the facts of this particular case, it is clear that any such program must also adopt controls covering how third party vendors may access, use, store and dispose of consumers' personal data.

Client Update:

SEC Issues Cybersecurity Guidance for Registered Investment Advisers and Funds

The SEC's Division of Investment Management has issued an IM Guidance Update addressing cybersecurity issues faced by registered investment advisers (including private fund managers) and registered investment companies (in plain English, "funds"). The IM Guidance Update makes plain that registered investment advisers and funds need to actively manage their cybersecurity risks – and be prepared to respond in the event of a cyberattack or data breach – or risk running afoul of the U.S. federal securities laws.[1]

In the Division's view, for example, failure to mitigate exposure to compliance risks associated with cyber threats through compliance policies and procedures could violate the rules under the U.S. Investment Advisers Act of 1940 and the U.S. Investment Company Act of 1940 that require registered investment advisers and funds to adopt and maintain written policies and procedures designed to assure compliance with federal securities laws. These rules also require annual reviews to ensure that the policies are adequate and effectively implemented. Similarly, the IM Guidance Update states that failure to mitigate harm from cyberattacks that expose personal identification information, or that prevent investors from exercising their legal rights (*e.g.*, where a shareholder in an open-ended fund is prevented from redeeming shares due to disruption from a cyberattack), could be construed as violations of the SEC's identity theft red flag rules or Section 22(e) of the Investment Company Act

[1] The full text of the guidance is available through the Investment Management Division webpage, http://www.sec.gov/investment, or in PDF format at http://www.sec.gov/investment/im-guidance-2015-02.pdf.

(in the event that a cyberattack prevents a fund from meeting redemption requests).

The IM Guidance Update thus reinforces a clear regulatory trend: cybersecurity standards that might previously have been seen simply as common sense or best IT practice can now, in effect, have the force of law.

RISK MITIGATION

The Division's views with respect to risk mitigation closely mirrors other leading cybersecurity standards, like the Framework issued by the National Institute of Standards and Technology. Specifically, the Division recommends that funds and investment advisers conduct periodic assessments of:

- where they store sensitive information (like Social Security numbers, bank account details, or passport information), and how they secure that information;
- what cybersecurity threats the firm faces, including both insiders (*e.g.*, the disgruntled employee) and outsiders (*e.g.*, hackers and other cybercriminals);
- how the firm's IT infrastructure may be vulnerable to those threats;
- what security controls and processes the firm has – or should – put into place to mitigate those threats;
- what impact a breach or disruption would have on the firm's systems, and what backups are in place to mitigate those effects; and
- how the firm's governance structure addresses and manages cybersecurity risk.

BREACH DETECTION AND RESPONSE

In addition to mitigating risks, the IM Guidance Update recognizes it is simply not possible to prevent every cyberattack. The Division's guidance indicates that registered funds and advisers should:

- Control access to firm systems, especially those that contain sensitive data, using both technical means (firewalls, strong user credentials like two-factor authentication) and employee training that reduces the possibility of insider attacks;
- Encrypt sensitive data wherever it exists on the firm's network, back up that data, and restrict the use of removable storage media (like USB thumb drives) that could lead to sensitive data moving outside the firm's control;
- Deploy software that monitors for unauthorized activity and other unusual events – and be sure to regularly update that software and the firm's knowledge base of what cyber threats are facing the financial services sector (*e.g.,* through participating in information-sharing groups like FS-ISAC);
- Develop a detailed incident response plan and test that plan regularly to ensure that it will be effective when a breach actually occurs; and
- Implement policies and procedures, and conduct regular training, to ensure that fund officers and employees understand cybersecurity risks and how to respond to incidents.

Good breach detection works best when good risk mitigation is already in place. Understanding where the adviser or fund stores sensitive information (mitigation) is a necessary step before securing that information and identifying intrusions (detection) is possible.

The IM Guidance Update notes that a firm's obligations in this regard don't stop at the front door. Nearly all registered funds and

investment advisers rely on third-party vendors and service providers to carry out their day-to-day operations – meaning a cyberattack on one of those third parties may have the same impact as an attack on the firm itself. The IM Guidance Update specifically highlights the importance of assessing vendors' cybersecurity policies and procedures, including by using contractual provisions to ensure a minimum level of compliance.

The IM Guidance Update, coupled with the recent report by the SEC's Office of Compliance Inspections and Examinations concerning its cybersecurity examination sweep, provides a roadmap for the policies and practices that funds and investment advisers should already be implementing with respect to cybersecurity mitigation and breach response.[2] Firms of every size and prominence are targets, although the nature of their risks may vary. While acknowledging that it is not possible for a fund or adviser to anticipate and prevent every cyberattack, the Division now has clearly communicated its expectations that firms will conduct thorough, thoughtful, and repeated assessments of what risks the firm faces, how to reduce those risks, and how to respond in the event of a breach or attack. By highlighting the risk that a firm could violate U.S. federal law if it fails to do so, the IM Guidance Update makes it clear that cybersecurity is not only an IT issue, it is also a compliance issue that should be on the minds of every officer and employee. Registered investment advisers, including private

---

[2] *See* OCIE Cybersecurity Examination Sweep Summary, National Exam Program Risk Alert, Vol. IV, Issue 4 (Feb. 3, 2015), http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf. We have also previously written about OCIE's priorities for 2015, in an update *available at* http://www.debevoise.com/insights/publications/2015/02/what-will-the-eyes-and-ears-of-the-sec-choose.

fund sponsors, should be proactive in identifying the cybersecurity risks of their business and reviewing their compliance policies and procedures to confirm that these risks are addressed.

This client update was originally issued on May 7, 2015.

Client Update:
DFS Expands Its Cyber Focus to Insurers

On Thursday, March 26, New York State's Department of Financial Services (DFS) announced a major expansion of its cybersecurity efforts: DFS will require insurers to respond to a special "comprehensive risk assessment" on cybersecurity, with those assessments to be followed by an enhanced focus on cybersecurity as part of DFS's regular examinations of insurers. DFS's announcement expands to insurance the increasingly rigorous approach it has recently applied to banks in the area of cybersecurity. More importantly, it offers critical guidance to all industries about what regulators will consider adequate precautions and preparation in this area.

THE DFS LETTER

The DFS action took the form of a so-called "308 letter" from Benjamin Lawsky, the DFS Superintendent, to CEOs, general counsels and CIOs of insurers. Section 308 of the New York Insurance Law gives DFS broad information-gathering powers. This 308 letter spells out the details of the one-time comprehensive risk assessment in the form of a detailed written questionnaire that must be answered by April 27. Insurers will have to answer questions about a broad range of cybersecurity issues – many of which mirror those that DFS required banks to answer in December 2014 – including:

- Corporate governance of cybersecurity, including the curriculum vitae and job description of the Chief Information Security Officer or other senior person responsible for cybersecurity;
- Policies and procedures designed to further the goals of confidentiality, integrity and availability of data, including the

integration of data classification (a/k/a the sorting of data according to its sensitivity and risk level) into such policies and procedures;
- Various highly specific security topics, such as the use of multi-factor authentication, patch management, penetration testing and vendor management. (N.B.: It is a matter of public record that criminals' abuse of credentials issued to third-party vendors has been implicated in a number of recent, high-profile hacks.);
- Steps taken to adhere to the Framework for Improving Critical Infrastructure Cybersecurity issued by the National Institute of Standards and Technology (NIST) on February 12, 2014 concerning third-party stakeholders;
- Policies and procedures governing relationships with third-party service providers that address information security risks;
- Protections used to safeguard sensitive data that is sent to, received from or accessible to third-party service providers, such as encryption or multi-factor authentication;
- Protections against loss or damage incurred as a result of an information security failure by a third-party service provider;
- Incident detection and response processes, including real-time monitoring and the institution's written incident response plan;
- Cyber insurance coverage; and
- Periodic reevaluation of policies and procedures in light of changing risks.

In the 308 letter, DFS notes its expectation that companies will make efforts to obtain any information necessary to respond to the questionnaire from parent or affiliate companies, and imposes upon parent companies the obligation to obtain such information from subsidiaries.

IMPLICATIONS FOR INSURERS AND OTHER COMPANIES

DFS has not promulgated specific cybersecurity standards, but it is strongly suggesting what it considers best practices by the questions it asks. We have previously called that "regulation by implication" – the questions themselves imply answers that the agency is likely to prefer. Strong substantive answers on the enumerated topics, clearly presented, can be expected to generate clean examination reports. Answers that DFS considers highly unsatisfactory, in contrast, could prompt DFS to pursue civil enforcement measures.

Take multi-factor authentication as an example. For the uninitiated, this is the practice of requiring more than a single username/password combination to access a computer system – for instance, use of a one-time code received via a token or text message in addition to a password is a common form of multi-factor authentication. No state or federal law expressly dictates the use of multi-factor authentication, but by asking companies to describe their practices in this area, DFS is clearly signaling that, going forward, it hopes to see companies adopt policies and procedures favoring multi-factor authentication. That is consistent with Superintendent Lawsky's comments, in a February 25 speech, that DFS was considering promulgating regulations mandating the use of multi-factor authentication because, according to Lawsky, single-factor authentication "should have been dead and buried many years ago," and "it is time that we bury it now."

Another example is the new requirement (not previously applied by DFS to banks) for institutions to describe steps they have taken to adhere to the Cybersecurity Framework promulgated by NIST. The NIST Framework does not have the force of law, though DFS's reliance on it is yet another indication that the standard is increasingly seen as the emerging gold standard of cybersecurity

benchmarks. Simply by asking about the NIST Framework, DFS nudges it toward preferred legal status. That being said, nothing in DFS's guidance suggests that alternative benchmarking tools like ISO or SANS are inadequate or flawed.

This approach of regulation-by-inquiry is reflected throughout the DFS guidance: Simply by asking pointed questions – about vendor management, patch management, the use of written incident response plans and so on – DFS is dropping strong hints as to what it will consider "right" answers in the context of the examinations it will conduct in 2015.

Although the most recent DFS guidance specifically applies only to the insurers it regulates, management and boards throughout corporate America would do well to study both this guidance and the guidance issued to banks in December 2014. Companies that suffer cybersecurity incidents increasingly are facing pressure to defend themselves – whether in private litigation or in regulatory enforcement actions. Companies in all industries thus may find the DFS "308 letter" a useful checklist for assessing their own cybersecurity posture.

This client update was originally issued on March 30, 2015.

Client Update:

New Cyber Guidance From NY DFS: A Possible Path To "Reasonable Security"

New York State's Department of Financial Services has spelled out a detailed list of issues it will cover in the new cybersecurity portion of its bank examinations. In a world where companies increasingly are said to have an affirmative legal obligation to maintain robust cybersecurity, a major regulator's views on exactly how to discharge that obligation bear close attention – not just by the financial institutions that DFS regulates, but by corporations generally.

The new guidance follows up on DFS's promise, in a report it issued earlier this year, that cybersecurity would become a topic in its bank examinations going forward. The top-level message, DFS says, is that cybersecurity should now be viewed "as an integral aspect of [financial institutions'] overall risk management strategy, rather than solely as a subset of information technology." The more granular mandate is that banks will have to answer questions about these issues, among others:

- corporate governance of cybersecurity, including the CV and job description of the Chief Information Security Officer or other senior responsible person;
- policies and procedures designed to further the goals of confidentiality, integrity and availability, including the integration of data classification (a/k/a, the sorting of data according to its sensitivity and risk level) into such policies and procedures;
- various highly specific security topics, such as the use of multi-factor authentication, patch management, penetration testing, and vendor management (N.B. – it is a matter of public record

that criminals' abuse of credentials issued to third-party vendors has been a factor recently in a number of high-profile hacks);
- incident detection and response processes, including monitoring and the organization's written incident response plan;
- cyber insurance coverage; and
- periodic reevaluation of policies and procedures in light of changing risks.

For the banks that will be subject to these DFS examinations, the December 10 memo obviously provides a roadmap of sorts. Strong substantive answers on the enumerated topics, clearly presented, can be expected to generate clean examination reports. Answers that DFS considers highly unsatisfactory, in contrast, could prompt DFS to exercise its authority to pursue civil enforcement measures. DFS's legal authority also includes the capacity to refer matters to criminal prosecution, though that seems unlikely in this context.

(Side note: Banks will want to think about how to present their answers to DFS not just clearly, but confidentially. The examination template calls for a good deal of sensitive information. DFS and its predecessor agencies historically have been generous in allowing regulated entities to claim exemption under New York's Freedom of Information Law for the materials they submit in examinations.)

From a more aerial view, DFS's new guidance might fairly be seen as "regulation by implication." That is - ***simply by requesting detail about the use of particular practices, DFS is sending clear signals as to what it regards as best practices***. And given that DFS examinations have the potential to trigger enforcement actions, the agency's preference for this or that practice can in substance come to have the force of law.

Take multi-factor authentication as an example. For the uninitiated, this is the practice of requiring a person to enter more than one sort of credential to access a computer system – say, both an alphanumeric password and a code from a token. No state or federal law expressly dictates the use of multi-factor authentication. But by asking companies to describe their practices in this area, DFS is clearly signaling that, going forward, it hopes to see companies adopt policies and procedures favoring multi-factor authentication.

This approach can be seen throughout the DFS guidance: Simply by asking pointed questions – about vendor management, patch management, the use of written incident response plans, and so on – DFS is dropping strong hints as to what it will consider "right" answers in the context of the examinations it will conduct in 2015. For now, the cyber examinations are limited to banks. It is our expectation that DFS will largely if not completely extend them as well to insurance companies, which DFS also regulates.

Corporations in general can take useful guidance from this as well. The DFS memo resonates with a variety of legal authorities that call on companies in all sectors of the economy to maintain so-called "reasonable security" – or face legal consequences for failing to do so. To name just a few examples:

- At the motion to dismiss stage, a Minnesota federal judge this month upheld common-law negligence claims brought against Target by banks affected by the retailer's data breach. The decision recognizes a legal duty of care, while leaving the particulars of what satisfies that duty to be defined down the road. (N.B. – Just yesterday, the same judge also allowed substantial parts of a consumer class action against Target to proceed. The judge dismissed the negligence claims for failure to

plead economic harm; the issue of whether Target owed consumers a duty was not before the court.)

- California's Data Safeguard Law, Cal. Civ. Code §§ 1798.81.5, requires companies to maintain "reasonable" data security measures – but does not spell out what those measures must be.
- The Federal Trade Commission is suing a number of prominent hacking victims on the grounds that their cybersecurity allegedly was so poor as to constitute an unfair business practice under Section 5 of the FTC Act, 15 U.S.C. § 45. In court challenges, the FTC thus far has prevailed in its view that substantive data security standards can be established case by case through enforcement actions, and need not be affirmatively stated by the agency.

Corporations of all types thus must consider this potential double whammy: On the one hand, "reasonable security" may be emerging as a legal standard. On the other hand, no court, regulator or legislature has yet laid out an explicit path to satisfying that standard.

In the search for a path, every breadcrumb dropped by a major player like DFS is important. Management and boards throughout corporate America thus would do well to study the DFS guidance, and ask themselves: If a regulator came calling, or we had to defend a post-data-breach negligence action in court, how would we answer the sort of questions that DFS plans to ask the banks?

This client update was originally issued on December 19, 2014.

Client Update:

Court Upholds FTC Cyber Authority; Recent FTC Guidance on Insider Breaches Looms Larger

THE THIRD CIRCUIT UPHOLDS THE FTC'S CYBERSECURITY ENFORCEMENT AUTHORITY

Section 5 of the FTC Act states broadly that "unfair" and "deceptive" business practices are illegal. For about ten years, the FTC has brought a host of enforcement cases in the cybersecurity area. In a nutshell, the Commission asserts in these cases that data security practices are "unfair" if they are substantively inadequate, and "deceptive" if they run contrary to a company's own public statements. But the FTC has not issued formal cybersecurity guidance through a rulemaking process.

Wyndham Hotels got hit with an FTC enforcement action after it experienced multiple data breaches in 2008 and 2009. Wyndham hit back with a legal challenge, asserting that the FTC lacked the authority to sue it for deficient cybersecurity practices.

Ruling on August 24, a three-judge panel of the Third Circuit unanimously sustained the FTC's authority to bring an enforcement action against Wyndham, affirming a ruling below out of the District of New Jersey. The panel held that inadequate cybersecurity measures and privacy policies could constitute "unfair practices" under the FTC Act. The panel stated that Wyndham could be liable for unfair practices violations even where the conduct of the hackers was criminal, so long as the cybersecurity intrusions were foreseeable—and, the panel noted, an unforeseeability argument "would be particularly implausible as to the second and third attacks."

In rejecting Wyndham's argument that the company had insufficient notice of the particular cybersecurity practices favored by the FTC, the Court pointed to materials like the FTC's complaints in earlier cybersecurity cases and to a cybersecurity guidebook issued by the FTC in 2007.

MORGAN STANLEY'S INSIDER BREACH

In light of the Third Circuit's emphasis on past FTC guidance, the FTC's recent announcement that it would *not* take enforcement action against Morgan Stanley is all the more timely and important.

In January 2015, Morgan Stanley announced that a financial advisor in its wealth management division had stolen client data for some 350,000 accounts, representing nearly 10% of the bank's wealth management clients. Almost none of the compromised accounts were the thief's particular clients. Following the breach, account names, numbers and other customer information relating to approximately 900 accounts appeared on public websites.

The FTC opened an investigation of Morgan Stanley's data security practices prior to the breach. But on August 10, 2015, the FTC's Bureau of Consumer Protection, Division of Privacy and Identity Protection, published a closing letter – that is, it publicly ended its investigation without taking enforcement action.

A closing letter is the FTC enforcement staff's way of saying to industry, "We're taking a pass in this specific case – but the rest of you are now on notice of our reasons, so next time we may not be so lenient."

WHAT MORGAN STANLEY DID RIGHT

In its closing letter, the FTC staff highlighted the key aspects of Morgan Stanley's data security program that contributed to the decision not to pursue enforcement action:

- **Morgan Stanley "implemented a policy allowing employees to access only the personal data for which they had a business need."** The thief was acting contrary to company policy by reaching for the data of clients he did not personally serve; this was viewed as important by FTC. To state the obvious, an employee who cannot get access to sensitive stuff in the first place cannot steal that stuff.
- **Morgan Stanley implemented technological tools to monitor "the size and frequency of data transfers by employees."** Such monitoring, done right, can help flag anomalous data flows that are indicative of a breach.
- **The company deployed tools to block employee access to high-risk applications and websites.** Many financial institutions and other organizations now restrict access to applications and sites that are seen as risky—in particular, webmail, social media and other potential exfiltration points for stolen data.
- **Morgan Stanley prohibited employees from using USB drives or other removable media.** Although Morgan Stanley's policy ultimately was not properly configured in this instance, the FTC may view the existence of such a policy as required going forward.
- **Morgan Stanley responded swiftly once it had notice of the breach.** The company reviewed and, where necessary, remediated its network security protections and policies. The company also identified and terminated the employee; promptly alerted law enforcement; worked to remove the compromised

data from the Internet; notified affected clients; and offered identity protection services to the clients. Given the FTC's praise for Morgan Stanley on these issues, companies are well advised to review, refresh and test their written incident response plans to see how they compare.

Insider or "Snowden" risk is widely viewed as one of the most daunting challenges in all of data security. After all, it is impossible to run a business without giving your employees liberal access to data and system resources. The closing letter is a reminder to companies in all industries that, however daunting the challenge may be, the FTC sees robust efforts to tackle Snowden risk as a legal requirement.

The closing letter specifically warns that "risks, technologies, and circumstances change over time," and that "companies must adjust security practices accordingly." For today, though, companies are well advised to carefully assess their own Snowden-risk mitigation strategies in light of the Morgan Stanley closing letter. A good approach is to ask with particularity not just "are we doing X?", but "how well are we doing X and are there gaps we need to close?". This approach should help position a company to receive the FTC's next closing letter, rather than its next lawsuit.

This client update was originally issued on August 25, 2015.

Assessing Your Cybersecurity Posture

"We understand you're not happy with our privacy policy."

Our earlier sections covered what happens when things go wrong and a data breach occurs. In this section, we profile two tools that can help companies begin to come to grips with and, in a practical way, begin to implement a robust cybersecurity program.

The first tool is the FFIEC Cybersecurity Assessment Tool, issued in late June 2015. At least one regulator – FFIEC member the Office of the Comptroller of the Currency – has announced that it will begin incorporating the Assessment Tool into cybersecurity examinations of regulated institutions.

The second tool is one that you likely have heard of: the NIST Cybersecurity Framework, which was first issued in February 2014. Since its introduction last year, the Framework has rapidly gained prominence and now is regularly cited as a robust cybersecurity benchmark that can be used by companies to help inform and guide the development of their cybersecurity programs.

What The FFIEC's New Cybersecurity Assessment Tool Means For You

On June 30 2015, the Federal Financial Institutions Examination Council (FFIEC) issued a Cybersecurity Assessment Tool. Although the tool is voluntary, the Office of the Comptroller of the Currency (OCC) announced that it would gradually be introducing the Assessment Tool in its examinations. The release of the Assessment Tool comes only a few months after the FFIEC released the results of an assessment it conducted into community financial institutions' cybersecurity preparedness, and joins a growing list of efforts by government regulators to escalate the intensity of their review of firms' cyber-preparedness. The tool, which is publicly available on the FFIEC's website, includes two self-assessment documents that the FFIEC encourages institutions to use to determine their "inherent risk profile" – the threats facing the firm based on its size, position, and services offered – as well as their "cybersecurity maturity" – how well-prepared the institution is to defend against cyberattacks.

THE INHERENT RISK PROFILE

Institutions cannot fully appreciate the strength of their defenses without first understanding the threats they face. The FFIEC recognizes this basic principle by focusing the first part of its Assessment Tool on the risks a given firm faces across five categories:

- **Technology**. Firms connect to the Internet and the outside world in a number of ways. Identifying where and how those connections are made, where data is stored, and employees' access points to firm information – including mobile access – is the first step in knowing what risks the firm faces.

- **Delivery Channels**. Financial firms interact with their customers in a variety of ways, from mobile apps to ATMs. The FFIEC notes that both the raw number of access points, as well as the number of different types of access, can increase an institution's risk.
- **Online Products**. Some institutions offer products that are inherently Internet-based, which can increase risk. These include payment services, peer-to-peer payments, wire transfers, and other online or mobile products. Risks may also come from a financial institution acting as a service provider or intermediary.
- **Organization**. One of the most common cybersecurity risks is the IT architecture bloat that frequently accompanies mergers – companies link two systems together without fully understanding every facet of the integration. In addition, the way that privileged accounts are managed and the way the IT environment is staffed can all contribute to an institution's risk.
- **External Threats**. The FFIEC and other regulators have repeatedly emphasized that institutions face different risks based on their size and prominence. Measuring the volume and type of attacks an institution has faced, regardless of whether those attacks were successful, provides a way of measuring the firm's overall risk profile.

The FFIEC's Assessment Tool asks institutions to measure their risk for a number of factors in each of these five categories on a spectrum from "least inherent risk" to "most inherent risk" in order to build an overall profile of the firm. Companies of varying size and technological sophistication, including both internal systems and the services and products offered to customers, will have varying inherent risk profiles. Notably, the inherent risk profile does not take into account mitigating controls. That is, it is an overall risk

assessment based on factors that attempt to be objective such as the number of unsecured external connections to a network; the number of third parties with access to internal systems; the number of network devices; and whether and to what extent the bank has a mobile presence.

CYBERSECURITY MATURITY

The second part of the FFIEC's Assessment Tool provides guidance on measuring the institution's maturity in dealing with five different aspects of cybersecurity preparedness that the Assessment Tool refers to as "Domains":

- **Risk Management and Oversight**. The FFIEC's tool first addresses factors relating to a firm's cybersecurity oversight. The tool focuses on planning and preparedness, along with governance of those plans and training to ensure employees understand the cybersecurity threats facing the firm.
- **Threat Intelligence and Collaboration**. Understanding the nature of cybersecurity threats is a complex challenge given the variety of bad actors – from hacktivists to cyber-criminals to nation states looking for a competitive advantage. The FFIEC emphasizes that firms should be monitoring and sharing information relating to cyber-threats facing both themselves and peer firms.
- **Controls**. The FFIEC's tool emphasizes three different kinds of internal controls used to protect assets and infrastructure: preventative controls, which deter attacks; detective controls, which identify anomalous events that may indicate an attack; and corrective controls, used to identify and mitigate vulnerabilities within the system.
- **External Dependency Management**. Cyberattacks commonly (though not exclusively) involve external connections to a firm's

systems. The FFIEC, like many other regulators, including the New York Department of Financial Services, emphasizes the importance of performing regular due diligence of third-party connections and accounts that grant access to a firm's systems.

- **Incident Management**. Cyber-attacks are rapidly becoming simply a part of life for financial institutions of all sizes. The final piece of the FFIEC's tool focuses on how firms respond to attacks – both successful and unsuccessful – and how they report attacks that have occurred to regulators and law enforcement.

This portion of the tool requires companies to select from a series of declarative statements about their cybersecurity programs in order to come up with a rating along a five-tiered spectrum that runs from "baseline" – following the minimum legal requirements – to "innovative" – firms that develop processes and controls specific to their firm and have a real-time handle on their cybersecurity threat profile. By way of example, the "Risk Management and Oversight" Domain asks banks to choose from one of the following statements about board involvement in cybersecurity governance (the resulting ratings are noted parenthetically):

- Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. (Baseline)
- At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. (Evolving)
- The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities. (Intermediate)

- The board or board committee approved cyber risk appetite statement is part of the enterprise-wide risk appetite statement. (Advanced)
- The board or an appropriate board committee discusses ways for management to develop cybersecurity improvements that may be adopted sector-wide. (Innovative)

The other statements contained in the Assessment Tool are similarly specific and detailed, and provide a fairly precise set of guidelines for what the FFIEC views as best practices when it comes to cybersecurity. For that reason, the Assessment Tool may be a valuable resource even for those companies who are not subject to FFIEC regulation.

Institutions cannot fully appreciate the strength of their defenses without first understanding the threats they face.

As to those banks that do fall under FFIEC regulation, the Assessment Tool and related User Guide will bear close study. While the Assessment Tool notes that there is no single expected maturity level for a given financial institution, it also sets forth an expectation that "[i]n general, as inherent risk rises, an institution's maturity levels should increase." That is, those institutions with information technology systems that have a greater inherent risk (*e.g.*, because they have a greater number of vendors or devices on their networks) will be expected to strive beyond a "baseline" maturity rating, and get themselves further up the spectrum towards an "innovative" cybersecurity program. The FFIEC has now issued fairly precise guidance for how to accomplish that goal.

The NIST Framework:
An Emerging Common Cybersecurity Standard

To address the risks posed by cyberattacks against companies vital to national and economic security, in February 2013 President Barack Obama issued an executive order "to enhance the security and resilience of the Nation's critical infrastructure." A central feature of that order was to direct the creation of a voluntary framework, developed through a collaborative dialogue between the public and private sector, by which organizations could evaluate their cyber preparedness. The National Institute of Standards and Technology's ("NIST") Cybersecurity Framework emerged one year later. The NIST Framework has rapidly gained prominence from companies and regulators as an emerging set of best practices in the cybersecurity area.

FRAMING THE CHALLENGE

The Framework is built upon risk management principles and is intended to be voluntary, flexible, technology neutral, and adaptable to organizations with different sizes and needs. The Framework is also crafted to be an ongoing and repeated process for companies continually to evaluate both their current and target cybersecurity state. One of the goals of the Framework is to establish a common language, allowing for greater collaboration both within the private sector and between the private sector and government.

The Framework is made up of three components: the Framework Core, Implementation Tiers, and a Framework Profile.

The Framework Core

The "Core" is a set of activities that provides a guide for companies to evaluate their current and target cybersecurity states. It comprises

four elements: Functions, Categories, Subcategories, and Informative References. The Functions organize cybersecurity activities at their highest level. These activities are Identify, Protect, Detect, Respond, and Recover:

- Identify – understanding an organization's risks and capabilities
- Protect – developing and implementing safeguards for critical infrastructure
- Detect – activities to identify active cybersecurity events
- Respond – creating actions to defeat active cybersecurity events
- Recover – ensuring resilience and restoration of capabilities or services impaired during a cybersecurity event

Each Function is intended to be performed concurrently in order to achieve a firm's cybersecurity goals. Each Function is then divided into Categories, Subcategories, and Informative References, each of which can be tailored to the individual cybersecurity needs of an organization. A visual representation of the Core provided by NIST is below:

Implementation Tiers

The Framework's Implementation Tiers provide a measure of the maturity level of a firm's cybersecurity posture. NIST has created four tiers to describe how well a company has implemented a cybersecurity plan for each of the Core subdivisions: Partial implementation (Tier 1), Risk Informed implementation (Tier 2), Repeatable implementation (Tier 3), and Adaptive implementation (Tier 4).

Tier 1 is the lowest level; it denotes a reactive security state, where firms act in a non-formalized and ad hoc fashion with little appreciation of their cybersecurity risk. Tier 2 subdivisions will reflect risk-aware standards, with practices approved at the highest levels but not implemented across all dimensions of the organization. Tier 3 security standards consist of repeatable policies that are formally approved and established organization-wide. At the optimal end of the spectrum, a Tier 4 state would be adaptive to changes in technology and tactics with established risk-informed cybersecurity policies and procedures. NIST recommends that at a minimum, all organizations move from Tier 1 to Tiers 2 or 3.

THE FRAMEWORK PROFILE

Organizations can use the Core and Tiers to craft their own tailored Framework Profile. Each firm's profile would be unique, taking into account their Core Function Categories and Subcategories, business requirements, risk tolerance, and resources. The Framework recognizes that cybersecurity needs will vary among industries and companies of differing size. The flexibility of the Framework is intended to provide a common language and systematic process that can be adapted to each individual need.

Profiles are intended to describe both current and target security states. The Target Profile evaluates an organization's cybersecurity needs by choosing an appropriate Tier for each Core Function Category and Subcategory. The Current Profile objectively evaluates the security states in these same areas as they exist at that point in time. By analyzing the gaps between Target and Current states, firms can prioritize their improvement opportunities, identify areas where they may be overextending resources, and then set goals to meet their cybersecurity needs. This process of improvement is intended to be continual to meet the changing dynamics of the cybersecurity field.

LEGAL IMPLICATIONS OF THE FRAMEWORK

Organizations could consider adopting the Framework to craft their cybersecurity policies and practices for reasons beyond its potential effectiveness. The Framework is currently voluntary, but it is quickly becoming the de facto cybersecurity standard in the governmental sector. Numerous federal agencies such as the Department of Treasury, the Department of Energy, and the FCC have begun to adopt the Framework. Additionally, numerous states have also begun to adopt the Framework, and the National Governors Association has issued a resource guide for additional states to implement it. As the standard becomes more prevalent in government, there is an increasing potential for it to be formalized into binding regulations for companies vital to national and economic security, and basic principles from the Framework have been emphasized in enforcement actions by both federal and state regulators.

By adopting the Framework earlier, organizations will be prepared for these possibilities. Adopting the Framework also potentially offers a legal defense in the event of a cybersecurity breach. Should

courts recognize the Framework as the standard it seems to be becoming, effective implementation by a company would provide an argument against negligence claims brought in the wake of a data breach.

The Framework is crafted to be an ongoing and repeated process for companies continually to evaluate both their current and target cybersecurity state.

While the Framework has received strong reviews in its favor from private sector companies such as PWC and Intel, it is still a work in progress. Because it is new, there are not yet any quantifiable studies demonstrating security improvement by the adoption of the Framework. And because it is a voluntary standard, the benefits of cooperation through a uniform language have not yet been realized. Nor does the Framework take into account the statutory, contractual, or regulatory obligations an organization may face. The Framework does provide a unique opportunity to standardize cybersecurity practices, and its first version embodies valuable first principles for companies to implement and monitor their cybersecurity compliance over time.

Cross-Border Issues

"User name and password?"

Cybersecurity and data privacy are not solely domestic concerns. In this section, we take a look at various cross-border issues that are practically inherent in cybersecurity and data privacy.

The first article deals with three distinct but related topics: the much-watched Microsoft warrant case in which the United States Government seeks to compel compliance with a warrant for emails Microsoft stores on servers abroad; the impact that Edward Snowden's disclosures continue to have on America's relationship

with the EU; and an important potential expansion of EU data privacy laws.

We also provide copies of our Client Updates on an important ruling by the French data protection authority regarding the right to be forgotten, as well as significant new cybersecurity sanctions authorized by President Obama.

Does Private Data Need a Passport to Travel Across Borders?

In the world of cross-border data privacy, this has been an active and challenging year. The Second Circuit is considering a lower court decision holding that the United States government can use a warrant to access private data stored abroad. The fallout from the Snowden disclosures has focused data protection authorities in the European Union on the U.S.-EU "Safe Harbor" Framework agreement that allows for the transfer of personal data from the EU to the U.S. for self-certifying businesses. Separately, the EU is in the final stages of overhauling its data privacy regulations in ways that will broaden protections for personal data and stiffen penalties for non-compliant businesses. Amid such developments, companies face multiple privacy laws that regulate cross-border transfer of data, often requiring both significant attention to compliance requirements and investment in the infrastructure necessary to secure personal data.

I. THE MICROSOFT WARRANT CASE

The Second Circuit will soon hear argument in a landmark case that tests the U.S. government's authority to reach data stored on foreign servers.

In 2014, Magistrate Judge Francis of the Southern District of New York held that a warrant seeking data stored on servers located in another country under the Electronic Communications Privacy Act, allows the government to obtain that data as long as the recipient of the warrant operates – and can access the data – within the U.S. District Judge Preska affirmed the ruling. The court therefore ordered Microsoft to disclose email communications on servers located in Ireland.

Microsoft has appealed, arguing that the U.S. law at issue – the Stored Communications Act – does not apply extraterritorially. The case highlights that U.S. law tends to focus on the location of the service provider, rather than on the location of the customer who provides the data (or whose customers are the data subjects), while European data protection regulation tends to focus on the privacy rights of individuals, whose data is at issue.

Dozens of technology and media companies, civil liberties organizations, the Irish government, and a German member of the European Parliament have filed amicus briefs in support of Microsoft. Oral argument is scheduled for September 9, 2015. Microsoft and its supporters have argued that Second Circuit affirmance could potentially reduce domestic and international trust in a U.S. company's ability to keep data private by moving it offshore, ostensibly beyond the reach of U.S. law. A ruling in the government's favor could directly affect companies that had hoped to compete in the cloud computing market by asserting that they maximize data protection by storing data outside the U.S. territory, and may hasten a trend among providers to use a form of open-key cryptography to encode their customers' communications.

II. SNOWDEN AND THE "SAFE HARBOR" ARRANGEMENTS

Under the US-EU Safe Harbor Framework, which was adopted in 2000, U.S. organizations may register with – and then annually self-certify to – the U.S. Department of Commerce that they protect the personal data of EU persons in ways that meet the requirements of the EU's 1995 Data Protection Directive. That certification, which is subject to enforcement by the Federal Trade Commission and other government agencies, is one means by which organizations can transfer personal data from the EU to the U.S. consistent with the

requirements of that Directive. Currently, more than four thousand organizations participate in the Safe Harbor arrangements.

In light of the Snowden disclosures, the European Court of Justice ("ECJ") is currently considering whether the Safe Harbor Framework violates the right to privacy articulated in the European Charter of Fundamental Rights. In addition, EU data protection authorities are reviewing the Framework's terms and been hoping to strengthen them through changes they have been negotiating with their U.S. counterpart. Suspension of the Framework, as some in the EU have threatened, could significantly affect the free flow of personal data to the U.S. from EU countries at this time; however, suspension of the Framework does not seem likely.

The Safe Harbor Framework is one way that U.S. businesses may legally transfer EU personal data to the U.S. Another, more common, way is for the companies sending and receiving EU personal data to enter into contractual clauses, the terms of which have been specified and standardized by the EU, for the trans-border processing and receipt of such data. These clauses and their requirements may be burdensome for smaller companies. Larger, multi-national enterprises may adopt Binding Corporate Rules ("BCRs") – internal rules that define their privacy protection policies – to satisfy the requirements of the Directive that enterprises receiving EU personal data provide adequate protection, but these can be burdensome.

III. STEPPING UP DATA PROTECTION IN EUROPE

The EU is set to expand its data privacy regulations to protect the data of customers of any company that offers goods or services to EU residents or monitors their behavior, regardless of the business's

location. The European Commission is now in the final stages of considering a General Data Protection Regulation ("GDPR"), which will impose a number of requirements on covered companies. Organizations with more than 250 employees will be required to appoint data protection officers. Companies will be required to develop specific plans to respond to data breaches and incorporate data protection and default privacy requirements into all new technologies, products and services. Further, companies will be required to obtain explicit and active consent from customers and employees before processing and transferring data out of the EU. Even with consent, the regulation is expected to limit the flexibility to transfer personal data. The potential costs of not complying with the new regulation, moreover, will be high: companies that fail to abide will face enhanced sanctions, of up to 5% of annual global turnover or $1,000,000, whichever is higher. The new regulations are also expected to result in a more efficient and regularized enforcement of the data protection regime.

At this point, it seems likely that the GDPR will be adopted in the first half of 2016 and will go into effect two years later.

NEXT STEPS ON THE HORIZON

Companies face a myriad of privacy laws that regulate cross-border data transfers and require large investments in administrative compliance and security infrastructure.

Amid all of the uncertainty resulting from the fast pace of data protection developments, the trend is clear: The European approach toward protecting personal data privacy is trending toward affording enhanced protections to such data, including by regulating more strictly the transfer of such data outside the EU, including to the U.S. Companies should stay apprised of these developments and prepare

for the GDPR. For example, they can devise a compliance strategy for transfers and storage of EU data, improve the transparency of their approach to transferring customer data, and revise their privacy policies and agreements for customers, employees and others whose personal data they collect and store.

Client Update:

A New Ruling by the French Data Protection Authority: Is the Right to Be Forgotten Crossing the Atlantic to the U.S.?

France's data protection authority, the *Commission Nationale de l'Informatique et des Libertés* ("CNIL"), has ordered Google to delist several third-party links from search results across all of Google's worldwide search websites – not only from its domains directed towards Europe, such as "google.fr," but also the main U.S. site at google.com, among others. This order follows a 2014 European Court of Justice ("ECJ") ruling that individuals have a "right to be forgotten." The proposed EU Data Protection Regulation will likely further strengthen and extend this right.

WHAT IS THE "RIGHT TO BE FORGOTTEN" IN THE EU CURRENTLY AND TO WHAT EXTENT CAN NATIONAL AUTHORITIES SANCTION NON-EUROPEAN COMPANIES?

The 2014 Google case[1] involved a subsidiary from Google located in Spain, and jurisdiction of the Spanish courts over Google's U.S. parent was anything but certain. In its ruling, the ECJ clearly stated that EU data protection rules are applicable regardless of the location of the company processing the data, so long as the company has a subsidiary or a branch in Europe. In the view of the ECJ, EU data protection rules are not only applicable to the search engine's EU subsidiaries, but also to its sites located outside the EU. Such an extended territorial reach of EU rules has been, and remains as of today, contested by Google, leading effectively to the CNIL's

---

1 Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=361347.

decision. The ECJ decision also confirmed that EU data protection rules were applicable to search engines, which were determined to fall within the definition of "controllers."[2]

The decision also held that, because individuals had the right to control search results directing readers to news stories or information about their lives under applicable data protection rules, they could request that these links be "delisted" from a search engine's results. The ruling does not affect the underlying news stories or other personal information, which remain accessible on the website that originally published them, and their removal from the original website would require separate proceedings. In addition, the ECJ held that the right to be forgotten is not absolute and must be balanced against the fundamental rights of others to freedom of expression. Indeed, the links in these search results may be delisted only to the extent that the underlying news story or website to which the search result refers is no longer relevant to the original purpose for which the personal information was collected and published.

So far, the ECJ decision has effectively left it to search engine operators to provide a procedure for delisting links in search results upon request from individuals, over which data protection authorities of the member states retain some control. Currently, an individual seeking delisting of a link to their personal information

[2] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data on the free movement of such data, Article 2(d).

may fill out a form made available on all major search engines.[3] However, no official criteria were published indicating when the provider would have to accept the delisting request. Unfortunately, the ECJ did not provide much guidance in its decision. Seeking to fill in this gap, the Article 29 Working Party[4] suggested that, in a case involving a request to remove such a link from the search engine's results, a court should consider: (i) the situation of the individual; (ii) the quality of the search data; and (iii) the place and method of the underlying publication.

In response to the ruling, Google has established an online form where individuals may request the delisting of search results from Google's applicable European domains that link to a news story or website containing the individual's personal information.[5] Google has reportedly received over 250,000 requests to remove such links since the ECJ's 2014 ruling.[6] Commentators have noted that Google

---

[3] Google regularly publishes statistics on the number of delisting requests received and their sources, but does not provide any number regarding the actual number of requests accepted.

[4] The Article 29 Working Party is a working group set up under Article 29 of the 1995 Directive on Data Protection to examine questions arising from the application of the directive and to propose relevant changes in its provisions to the European Commission.

[5] The form is available at https://support.google.com/legal/contact/lr_eudpa?product=websearch.

[6] *See Europe's Expanding 'Right to Be Forgotten'*, NEW YORK TIMES (Feb. 4, 2015), *available at* http://www.nytimes.com/2015/02/04/opinion/europes-expanding-right-to-be-forgotten.html.

has only delisted around 40% of these requests and has not offered transparency in its criteria for making these decisions.[7]

U.S. courts, by contrast, are expected to be reluctant to follow suit. U.S. courts so far have been wary of placing an individual's privacy rights above the First Amendment's protections for historical reporting and dissemination of factual information. While there is no decision in place dealing with the delisting of links to information like in the ECJ case, the decision in the *Hearst* case is a reasonable indicator where U.S. courts are coming from: The U.S. Court of Appeals for the Second Circuit held that a newspaper was not required to remove stories about a woman's arrest, even though the arrest was later expunged from her record.[8] In so holding, the judge observed that the expunged record is a legal fiction that "does not and cannot undo historical facts or convert once-true facts into falsehoods."[9] Although in a recent defamation case before a New York state trial court, a judge commented that a statutory "right to be forgotten" would, "under certain conditions, [give] plaintiffs the opportunity to attain the redress they deserve,"[10] the comment remains an outlier without precedential effect.

---

7 For example, a number of academics have signed a letter to Google asking for further transparency around its treatment of these requests. *See Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data*, *available at* https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd.

8 *Martin v. Hearst Corp.*, 777 F.3d 546, 552 (2d Cir. 2015).

9 *Id.* at 551.

10 *Anonymous v. Does*, 151769/2013 (NY Sup. December 3, 2014) *4.

HOW DID THE GOOGLE CASE SET THE STAGE FOR EXTRA-TERRITORIAL ENFORCEMENT OF EU DATA PROTECTION LAWS IN THE UNITED STATES AND ELSEWHERE?

On May 21, 2015, the CNIL[11] decided to open a formal proceeding[12] against Google concerning the company's non-compliance with French data protection law. Google had displayed search results, as well as EU subsidiary-arranged advertising links, that related to the searched terms that had been the subject of delisting requests. The CNIL determined that Google fell under the authority of EU data protection regulators.

Following numerous complaints from people who had applied without success to delist the links referring to websites with their personal information from Google's search engine, the CNIL had asked Google to delist these links for 21 such individuals. Google ultimately complied with nine of these requests, but limited the removal to the search results appearing on its French domain "google.fr."

The CNIL then ordered Google to delist these results from all of the company's search engine's domains, including its non-EU domains such as "google.com." Although Google did so for its other European domains, it continued to refuse to delist the search results at issue for its domains outside the EU, which – according to Google – are not widely used within Europe.[13] Consequently, the CNIL decided to

---

11 *See* Commission Nationale de l'Informatique et des Libertés decision No. 2015-047, May 21, 2015.

12 The CNIL decision is in particular based on: (i) the French Law No 78-71 [1978], *loi relative à l'informatique, aux fichiers et aux libertés*; and (ii) the ECJ decision C131/12 [2014], *Google Spain SL v. Agencia Española de Protección de Datos*.

13 *See* Google's answer to the CNIL, letter dated April 24, 2015.

pursue the company for non-compliance with French data protection rules.

If Google does not comply with the request from the French authority, the CNIL will be in a position to levy sanctions of up to € 300,000 against the company for violation of the French data protection law.[14]

IS THE GOOGLE CASE JUST AN ISOLATED COURT DECISION, OR DOES THIS HERALD LARGER CHANGES IN EU PRIVACY AND DATA PROTECTION LAWS?

The Google case is illustrative of current trends in European data protection litigation and enforcement: for example, a lawsuit was recently brought in Belgium accusing Facebook of breaching European data privacy laws, and Germany has ordered Google to change the way it collects and combines its user data. Similar cases are to be expected in the near future, especially now that the EU is currently reforming its legislation concerning the protection and privacy of personal data.

On June 15, 2015, Ministers of the Council of the European Union determined a general approach to the reform proposal relating to the Draft on Data Protection Regulation.[15] Negotiations between the European Parliament and Council will start on June 24, 2015, with the aim to reach an agreement before the end of the year.

---

14 *Loi No 78-71 relative à l'informatique et aux libertés*, Article 47.

15 The Regulation will be accompanied by an EU Directive applying to general data protection principles and rules for police and judicial cooperation in criminal matters, for both domestic and cross-border transfer of data.

The proposed Data Protection Regulation[16] would likely strengthen and extend the right to be forgotten and could impose sweeping changes to the EU data protection landscape, affecting EU and global companies alike:

- *Harmonization and expansion of regulations.* The proposal introduces a single set of rules on data protection across the EU, also applicable to non-European companies, when they offer goods or services to EU residents or when monitoring their behavior (Article 3.2). A fine of up to 2% of annual worldwide turnover could be imposed on companies that do not comply with these rules (Article 79).
- *Increased accountability for data security.* The proposal would also heighten responsibility and accountability for the processing of personal data. For example, companies and organizations will be obligated to notify the national supervisory authority immediately of a serious breach of personal data (Article 31).
- *Role of national data protection authorities.* The proposal also introduces the possibility for EU organizations to deal exclusively with the national data protection authority of the member state in which they have their principal place of business (Article 48). Individuals could similarly refer complaints to the data protection authority in their country, even if their data is processed by a company located outside the EU.

---

16 Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on free movement of such data, COM(2012) 11 final, 2012/011 (COD) [2012].

- *Limitations on data privacy.* Some limitations on individuals' data privacy are nonetheless included in the proposal, including, for example, exceptions to protect public security or the rights or freedoms of others (Article 48).

The EU's latest proposal represents a new legal framework for the unified protection of personal data in member states. National legislatures across Europe are also moving towards stricter regulation of personal data protection.[17] As technology continues to develop and the need for new methods of personal data protection increases, additional regulations are likely to follow.

This client update was originally issued on June 24, 2015.

[17] For example, in Germany, a draft law (*Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts*) was adopted on February 4, 2015 to improve consumer protection by enabling particular protection organizations and trade associations to file injunctions against companies violating data protection provisions for consumers.

Client Update:

U.S. Authorizes Cyber Sanctions, Recommends Tech Companies Adopt Compliance Programs

On April 1, 2015, President Obama issued Executive Order (E.O.) 13694, authorizing new blocking sanctions (asset freezes) against persons that engage in certain significant and malicious cyber-enabled activities that threaten the United States.

Pursuant to the Executive Order, the Treasury Secretary, in consultation with the U.S. Attorney General and the Secretary of State, may impose sanctions on any individual or entity that engages in cyber-enabled activities "originating from, or directed by persons located, in whole or in substantial part, outside the United States" that cause, or seek to cause, significant harm or disruption to computers, computer networks or any of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21 (*i.e.*, the 2013 directive on Critical Infrastructure Security and Resilience). Additionally, E.O. 13694 authorizes sanctions against persons that steal significant funds, trade secrets or other personal or financial information, as well as those that knowingly receive or make use such stolen information.

No persons have yet been designated under the Executive Order, but those designated will be added to the Office of Foreign Assets Control's ("OFAC") list of Specially Designated Nationals and Blocked Persons. In the meantime, and concurrent with the issuance of the Executive Order, OFAC issued a list of Frequently Asked Questions ("FAQs").

In those FAQs, OFAC reminds U.S. persons (and persons otherwise subject to OFAC jurisdiction) that they must ensure they are not

engaging in transactions with any persons named under the Executive Order. To this end, OFAC specifically calls on "firms that facilitate or engage in online commerce" and other technology companies to develop "a tailored, risk-based compliance program, which may include sanctions list screening or other appropriate measures."

Until now, the U.S. government has focused principally on the need for banks and other financial services companies to have robust sanctions programs. This FAQ appears to be the first time that U.S. authorities have expressly voiced an expectation that technology companies should develop and implement sanctions-specific compliance regimes. It may be prudent for technology companies to review their sanctions-related risks and consider enhancing their compliance programs accordingly.

For technology and e-commerce companies, designing and implementing a risk-based sanctions compliance program – or enhancing an existing program – may present unique challenges. Many such companies have global user bases and operate under business models in which they may not readily be able to identify and verify the identity of customers, independent contractors, users and other counterparties prior to the provision of services. OFAC's recent $7.7 million settlement with PayPal, Inc. ("PayPal") highlights the importance of designing and implementing effective sanctions compliance programs. The settlement agreement suggests PayPal failed to maintain adequate sanctions screening and monitoring procedures and consequently processed transactions in apparent violation of U.S. sanctions related to Cuba, Iran, Sudan, global terrorism and the nonproliferation of weapons of mass destruction.

E.O. 13694 is the latest development in the U.S. government's use of sanctions to deter and punish global cyber-crimes. Earlier this year, President Obama issued E.O. 13687, authorizing expanded sanctions on North Korea's government in response to the cyber-attack on Sony Pictures Entertainment, among other provocations. In December, Section 1637 of the National Defense Authorization Act for fiscal year 2015 authorized the President to impose blocking sanctions on any non-U.S. person determined to knowingly support, facilitate or benefit from the "significant appropriation," through espionage in cyberspace, of U.S. technologies or proprietary information. Pub. L. No. 113-291, 128 Stat. 3292.

This client update was originally issued on April 6, 2015.

Federal Legislation Update

"Just for kicks, Leon, let's shut down the F.B.I. again."

We close this first edition of *Breach Reading* with an overview of pending federal cybersecurity legislation. One of the challenges in doing any review of the law in this space is the speed with which it is changing. As we drafted this book, we periodically refreshed this article in an effort to keep it current. What we share here is a state of the law (pending and otherwise) as it existed in August 2015. Given the speed with which things move in this space, however, we caution that by the time you are reading this, the world might look very different. That being said, we sincerely hope you found our

summary – and this inaugural edition of *Breach Reading* – a valuable resource.

Wading Through the Waves of Pending Federal Cybersecurity Legislation

Since January 2015, members of the House and Senate have introduced several bills that seek to legislate how businesses and other organizations respond to cybersecurity breaches. Most of the bills fall into one of two groups. First, several bills address information sharing between private organizations and the federal government in connection with cybersecurity threats. Second is a series of bills that address notification requirements when sensitive information is stolen in a data breach.

I. INFORMATION SHARING BILLS

Five bills currently pending in Congress seek to promote information sharing between private entities and the government. Two of these bills, the Protecting Cyber Networks Act ("PCNA") and the National Cybersecurity Protection Advancement Act ("NCPAA"), passed the House in April 2015 and were combined into a single bill that is currently awaiting a vote in the Senate.

Both bills amend existing legislation to permit private entities to share information about cybersecurity threats with other private entities and with certain government agencies. Private entities would be permitted to monitor information systems under certain circumstances and in some instances take defensive measures. A key provision of both bills is that companies that choose to share information would be protected from liability for sharing that information with the government, notwithstanding any other provision of the law. Some state laws might otherwise impose liability for this type of information sharing.

PCNA VS NCPAA

	PCNA	NCPAA
Monitoring	Private entities may monitor information systems of any private or government entity that provides written consent. Private entity that detects a threat may conduct a "defensive measure" to defeat it regardless of where it originates, but may only destroy a system it has consent to monitor.	Private entities may monitor information systems of any private or government entity that provides written consent. Private entity that detects a threat may conduct a "defensive measure" to defeat it, regardless of where it originates, but may only destroy a system it has consent to monitor.
Parties Permitted to Share Information With	Private Entities Appropriate federal agencies, including: Department of Commerce; Department of Energy; Department of Homeland Security; Department of Justice; Department of Treasury; and Office of the Director of National Intelligence	Private Entities Department of Homeland Security's National Cybersecurity and Communications Integration Center (the "Center")
Liability Protection	Entity shielded from liability for sharing information notwithstanding any other provision of law. Does not constitute waiver of any applicable privilege or protection provided by law, including trade secret protection.	
Conditions on Liability Protection	Must utilize a security protocol designed to protect against unauthorized access to any cybersecurity threat information. Must take reasonable efforts to remove PII not directly related to the cybersecurity threat.	Must implement appropriate security controls to protect against unauthorized access to cybersecurity threat information. Must take reasonable efforts to remove PII not directly related to the cybersecurity threat.

	PCNA	NCPAA
How Federal Government Permitted to Use Information	For a "cybersecurity purpose" meaning to protect (including through the use of a defensive measure) an information system or information that is stored on, processed by, or transiting an information system, or to identify the source of a cybersecurity threat To prevent or investigate a threat of death or serious bodily harm or any offense arising out of the threat To prevent a serious threat to a minor To prevent certain statutorily enumerated offenses	For a "cybersecurity purpose" meaning to protect an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity risk or incident, or to identify the source of a cybersecurity risk or incident Expressly prohibited from using information for regulatory purposes

Three similar bills are currently pending in committee in Congress. These bills would make changes like the PCNA and the NCPAA, but with some key differences. The Cyber Threat Sharing Act of 2015 ("CTSA") requires private entities to certify compliance with Department of Homeland Security ("DHS") best practices if it shares information with a private Information Sharing and Analysis Organization. The Cybersecurity Information Sharing Act of 2015 ("CISA") would shield companies from liability for sharing information so long as they comply with a DHS-defined process for doing so. Finally, the Cyber Intelligence Sharing and Protection Act ("CISPA") would allow federal agencies to share cybersecurity threat information with any private cybersecurity provider and any entity that provides cybersecurity services to itself as long as they possess certain security clearances.

Before Congress' August recess, there was some activity around bringing CISA to the Senate floor. However, procedural concerns regarding potential amendments led the Senate to adjourn for August without actually opening debate on the bill, though it may be revived in the fall. In general, the fate of CISA – like others before it – remains uncertain as the Senate has other significant business before the coming election season.

II. BREACH NOTIFICATION

Six bills, versions of which are pending in House and Senate committees, seek to establish a national standard for informing consumers after a security breach. All would explicitly preempt the roughly four dozen state laws that currently govern when and how companies must make notifications about data breaches.

The bills function in essentially the same way. After a security breach, covered entities would be given a certain number of days to inform people and government entities of the breach. Notice could be provided in writing, by email, or by telephone. Generally, the notice would have to include: (1) a description of the compromised information; (2) a toll-free number that the person can use to contact the breached company; and (3) toll-free phone numbers for the major credit reporting agencies and the FTC.

NOTICE AND INFORMATION REQUIREMENTS

	Personal Data Notification Protection Act of 2015 ("PDNPA")	Data Security and Breach Notification Act of 2015 ("DSBNA")	Data Security Act of 2015 ("DSA")
Timing of notice	Without unreasonable delay following discovery of breach	Within 30 days of discovering breach	Without unreasonable delay following discovery of breach
Required information	1. Description of compromised PII 2. Contact information to find out about breach and type of information the business possessed 3. Contact information for major credit reporting agencies and FTC 3. Name of business breached 4. State-required information regarding victim protection assistance (*e.g.* right to obtain police report, how to request a security freeze and information required to do so (MA))	1. Description of compromised PII 2. Contact information to find out about breach and type of information the business possessed 3. Contact information for major credit reporting agencies and FTC 4. Contact information to obtain material about identity theft from FTC 5. Notice that person may be entitled to consumer credit reports 6. Instructions on how to obtain consumer report 7. Date of breach	1. Description of compromised PII 2. Description of actions taken to restore security 3. FTC summary of rights for victims of identity theft

NOTICE AND INFORMATION REQUIREMENTS

	Data Breach Notification and Punishing Cyber Criminals Act of 2015 ("DBNPCCA")	Cyber Privacy Fortification Act of 2015 ("CPFA")	Data Accountability and Trust Act ("DATA")
Timing of notice	Within 30 days of discovering breach	Prompt notice after discovering breach	Within 45 days of discovering breach
Required information	1. Description of compromised PII 2. Contact information to find out about breach and type of information the business possessed 3. Description of how breach occurred 4. Date of breach	1. Information surrounding breach	1. Description of compromised PII 2. Contact information to find out about breach and type of information business possessed 3. Contact information for major consumer credit reporting agencies 4. Contact information to obtain material about identity theft from FTC 4. Notice that person may be entitled to two years of credit reports or credit monitoring

All of the bills except for the CPFA require notice to consumers, the FTC, and one or more of the following entities if a certain threshold number of individuals are affected by the breach:

- National consumer credit reporting agencies
- Federal entity designated by DHS

- Appropriate federal law enforcement agency (*e.g.* FBI, Secret Service)

The CPFA is an outlier. Under the CPFA, an entity is not required to notify consumers or the FTC, but it requires entities to notify the Secret Service or the FBI.

WHOM TO NOTIFY

	PDNPA	DSBNA	DSA
Notice to consumers?	Yes	Yes	Yes
Notice to FTC?	Yes	Yes	Maybe
Notice to credit reporting agencies?	Yes, if more than 5,000 people notified	Yes, if more than 5,000 people notified; must provide credit reports for two years	Yes, if more than 5,000 people notified
Notice to other organizations?	Must notify entity designated by DHS if: 1. PII of more than 5,000 people accessed or acquired; 2. Breach involves PII database of more than 500,000 people; 3. Breach involves a database owned by the federal government; and 4. Breach involves PII of federal government employees involved in national security or law enforcement.	Must notify entity designated by DHS if: 1. PII of more than 10,000 people was accessed or acquired; 2. Breach involves PII database of more than 1,000,000 people; 3. Breach involves a database owned by the federal government; and 4. Breach involves PII of federal government employees involved in national security or law enforcement	Must notify: 1. Appropriate federal law enforcement agency 2. Appropriate agency as defined by the bill 3. Any relevant payment card network

WHOM TO NOTIFY

	DBNPCCA	CPFA	DATA
Notice to consumers?	Yes	No	Yes
Notice to FTC?	Yes	No	Yes
Notice to credit reporting agencies?	No	No	Yes; must provide credit reports/credit monitoring for two years if requested
Notice to other organizations?	Must notify entity designated by DHS if: 1. PII of more than 1,000 people accessed or acquired; 2. Breach involves PII database of more than 250,000 people; 3. Breach involves a database owned by the federal government; and 4. Breach involves PII of federal government employees involved in national security or law enforcement	Must notify Secret Service or FBI	No

All of the pending bills exempt entities from the individual notice requirements in certain circumstances. Some permit a company to forego notice if it conducts a risk assessment and determines that

there is no "reasonable risk" that consumers will be harmed. Others define a data breach to exclude instances where the accessed data is encrypted or unusable. A company also could be permitted to delay notice by law enforcement agencies to protect national security or an ongoing investigation. Some bills would exempt a business from the notice requirement if it uses a security program that blocks the use of sensitive PII to initiate unauthorized financial transactions.

CIRCUMSTANCES IN WHICH ENTITY EXEMPT FROM INDIVIDUAL NOTICE REQUIREMENT

	PDNPA	DSBNA	DSA
Risk assessment determines no "reasonable risk" consumers will be harmed	Yes Rebuttable presumption no harm will result if data was encrypted or unusable	Yes Rebuttable presumption no harm will result if data was encrypted or unusable	No
Encrypted or unusable data excluded from definition of security breach	No	No	Yes
Notification delayed for law enforcement or national security purposes	Yes	No	No
Security program blocks unauthorized use of PII to initiate unauthorized financial transactions	Yes Must notify affected individuals after a security breach that results in an unauthorized transaction	Yes Must notify affected individuals after a security breach that results in an unauthorized transaction	No

CIRCUMSTANCES IN WHICH ENTITY EXEMPT FROM INDIVIDUAL NOTICE REQUIREMENT

	DBNPCCA	CPFA	DATA
Risk assessment determines no "reasonable risk" consumers will be harmed	No	No	Yes Rebuttable presumption no harm will result if data was encrypted or unusable
Encrypted or unusable data excluded from definition of security breach	Yes	No	No
Notification delayed for law enforcement or national security purposes	Yes	No	Yes
Security program blocks unauthorized use of PII to initiate unauthorized financial transactions	No	No	No

Under a majority of the pending bills, enforcement would be left to the FTC and/or State Attorneys General. The DSA would allow for enforcement by the US Attorney General and for a private right of action for knowing and negligent violations. Additionally, two bills would allow for fines and/or imprisonment for parties who knowingly fail to provide notice or willfully conceal a breach.

ENFORCEMENT AND DAMAGES

Enforcement	**PDNPA**	**DSBNA**	**DSA**
FTC	Yes	Yes	Yes (Administrative)
State Attorneys General	Yes	Yes	No
US Attorney General	No	No	Yes
Damages			
Private Right of Action	No	No	Yes Damages, costs, attorney's fees, and, for knowing violations, punitive damages
Cap on Damages	$1,000,000, unless violation willful or intentional.	$5,000,000 (individual notice) $1,000,000 for failing to notify the federal government.	None
Fines/Imprisonment	No	Fines and up to five years imprisonment for willful and intentional concealment when harm more than $1,000	No

ENFORCEMENT AND DAMAGES

Enforcement	DBNPCCA	CPFA	DATA
FTC	Yes	No	Yes
State Attorneys General	Yes	Yes	Yes
US Attorney General	No	No	No
Damages			
Private Right of Action	No	No	No
Cap on Damages	$1,000,000	$500,000 $1,000,000 for intentional violations	$5,000,000
Fines/Imprisonment	No	Fines and up to five years imprisonment for knowing failure to provide notice of a security breach	No

In addition to standardizing notice requirements, the DSBNA, DSA, DBNPCCA and DATA would require covered entities to establish and implement policies to protect PII. The DSA has the most stringent requirements because a covered entity's board of directors would have to oversee and approve the program. Failure to implement these policies could result in civil penalties.

CYBERSECURITY PROGRAM REQUIREMENTS

PDNPA	DSBNA	DSA
None	Company must: 1. Implement a policy with respect to the collection, use, sale, other dissemination and maintenance of PII; 2. Identify an employee to serve as the manager of information security; 3. Develop an audit system to detect vulnerabilities; 4. Correct any detected vulnerabilities; and 5. Develop a process for disposing of PII	Company must: 1. Designate an employee to coordinate the program; 2. Develop a system to identify internal and external threats to information safety; 3. Design a system to mitigate the risks identified; and 4. Ensure service providers have systems in place to protect PII. If a covered entity has a board of directors, the board must oversee the development of the policy and approve it

CYBERSECURITY PROGRAM REQUIREMENTS

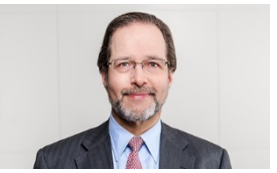
DBNPCCA	CPFA	DATA
Covered entity must take reasonable measures to protect and secure PII	None	Company must: 1. Implement a policy with respect to the collection, use, sale, other dissemination and maintenance of PII; 2. Identify an employee to serve as the manager of information security; 3. Develop an audit system to detect vulnerabilities; 4. Correct any detected vulnerabilities; and 5. Develop a process for disposing of PII

CONCLUSION

The bills function in essentially the same way: after a security breach, covered entities are given a certain number of days to inform people and government entities of the breach.

While it is difficult to know whether any of the bills will become law, understanding the range of proposals can help companies anticipate what future cybersecurity requirements might look like, and what regulators might deem as "reasonable" cybersecurity measures. Whatever the outcome of the pending legislation, these bills almost assuredly will not be Congress's last attempt to bring more order to our nation's cybersecurity regulatory scheme.

Contributors

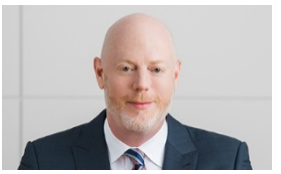


JEFFREY P. CUNARD

Jeffrey Cunard is a corporate partner who leads the firm's corporate intellectual property, information technology and e-commerce practices. He has broad experience in transactions, including software and technology licenses, joint ventures, mergers and acquisitions, and outsourcing arrangements. Mr. Cunard's practice additionally involves copyright litigation and he is a member of the firm's Cybersecurity & Data Privacy practice. He advises in U.S. and international media and telecommunications law, including privatizations and regulatory advice.

JEREMY FEIGELSON

Jeremy Feigelson is a litigation partner in the firm's Intellectual Property Group and leads the firm's Cybersecurity & Data Privacy practice. He frequently represents clients in litigations and government investigations that involve the Internet and new technologies. His practice includes litigation and counseling on privacy, trademark, false advertising, copyright and defamation matters. Mr. Feigelson also has a broad and active practice in financial services matters, including securities litigation, investment management disputes and counseling of fund boards, the conduct of internal reviews, defense of government investigations and complex commercial litigation.



MICHAEL P. HARRELL

Michael Harrell is a corporate partner and member of the firm's global Private Equity and Investment Management Groups. Mr. Harrell has advised some of the private equity industry's leading sponsors of buyout, growth capital, distressed debt, media and telecommunications, international private equity, mezzanine and other U.S. and non-U.S. private investment funds. He currently represents the Private Equity Growth Capital Council with respect to legal developments affecting the private equity industry globally.

DAVID A. O'NEIL

David O'Neil is a litigation partner and member of the firm's White Collar & Regulatory Defense Group and Cybersecurity & Data Privacy practice. His practice focuses on white collar criminal defense, internal investigations, privacy and cyber security, congressional investigations, and AML/sanctions enforcement defense. Prior to joining Debevoise 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.

JIM PASTORE

Jim Pastore is a litigation partner and a member of the firm's Cybersecurity & Data Privacy practice and Intellectual Property Group. His practice focuses on privacy and cybersecurity issues. Prior to rejoining Debevoise in 2014, Mr. Pastore served for 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.

Acknowledgements

The authors would like to thank Debevoise associates Christopher S. Ford, Anna Gressel, Justin Horton, and Olena Ripnick-O'Farrell for their invaluable contributions to this inaugural edition of Breach Reading, including their research, drafting, and revising of the materials. A special thank you to Yolanda Cartusciello, Fred Loessel, Christopher W. Sexton, Kate Zvonkovic, Richard Fitch, 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 Sydney Egnasko, Brandon Fetzer, Isabela Mazzola Garcez, Rhianna M. Hoover, Taylor M. Lindman, Andrew L. Mandelbaum, Ryan Mullally, and Joshua Smith. We appreciate all the hard work.