July 2015

Skadden

Privacy & Cybersecurity Update

Seventh Circuit Decision May Make It Easier for Class Action Plaintiffs to Establish Standing in Data Breach Cases

The Seventh Circuit has issued a decision that could make it much easier for class action plaintiffs to establish standing without showing actual identity theft or other misuse of personal information. If the court's rationale is followed in other circuits, the decision could significantly alter the landscape for class action claims arising from data breaches.

On July 20, 2015, the U.S. Court of Appeals for the Seventh Circuit issued an important ruling regarding standing in data breach cases that could potentially have a dramatic impact on whether these cases survive motions to dismiss for lack of standing. Specifically, the ruling could make it easier for data breach class action plaintiffs to establish standing without showing actual identity theft or other misuse of their personal information.

In *Remijas v. Neiman Marcus Group, LLC,*[1] the Seventh Circuit reversed the district court's dismissal of the plaintiffs' putative class action complaint, holding that plaintiffs had, in fact, sufficiently established standing under Article III. The Seventh Circuit is the first federal appellate court to address the holding of the U.S. Supreme Court in *Clapper v. Amnesty Int'l USA*[2] that the alleged injury must be "certainly impending" to be sufficiently concrete and imminent to establish Article III standing.

Background

Neiman Marcus is a high-end retail store specializing in designer apparel. At the height of the holiday shopping season in 2013, hackers installed malware on Neiman Marcus computers. The malware exposed up to 350,000 credit card numbers of Neiman Marcus customers, 9,200 of which were then used fraudulently. Neiman Marcus learned of the existence of malware on its computer systems on January 1, 2014, and disclosed the data breach nine days later. The disclosures prompted the filing of class action complaints that were then consolidated into one complaint alleging claims of negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy and violation of multiple state data breach laws.

[1] No. 14-3122, 2015 WL 4394814 (7th Cir. July 20, 2015).

[2] 133 S. Ct. 1138, 1147 (2013) (instructing that future harm must be "certainly impending" and holding that "allegations of possible future injury are not sufficient").

Plaintiffs' Claims

In their suit, the plaintiffs made the types of claims that have been common in data breach cases, alleging that they suffered:

- lost time and money resolving the fraudulent charges;
- lost time and money protecting themselves against future identity theft;
- the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity; and
- lost control over the value of their personal information.

The plaintiffs did not allege that any fraudulent charges had not been reimbursed by the credit card companies.

The plaintiffs also alleged that they suffered two future "imminent injuries":

- an increased risk of future fraudulent charges; and
- greater susceptibility to identity theft.

The district court dismissed the class action on the grounds that the plaintiffs failed to allege sufficiently concrete and particularized injury under *Clapper*.

Seventh Circuit Ruling

The Seventh Circuit reversed the district court and remanded for further proceedings. The court noted that *Clapper* did not foreclose all future injuries as grounds for Article III standing. Instead, the court held that, where the presumed purpose of the hackers' theft of consumers' private information is to make fraudulent charges or steal consumers' identities, the plaintiffs should not be required to wait until such events occur. The court found that the plaintiffs had pled a "substantial risk of harm" from the data breach sufficient to confer class standing.

Interestingly, the court used Neiman Marcus' offer of one year of credit-monitoring services to all affected customers against the company. Though now a common practice among companies that suffer data breaches, the court used the offer as evidence that Neiman Marcus itself believed that the risk of identity theft was significant enough to warrant the costs of the credit monitoring services. Based in part on this reasoning, the court found the plaintiffs' allegations of lost value of time spent resolving fraudulent charges and costs for credit monitoring services to prevent future identity theft sufficiently "concrete" for standing.

Court Declined to Rule on Two Types of Injury

In its decision, the Seventh Circuit declined to rule on two categories of alleged injuries asserted by the plaintiffs, noting that it was "dubious" they would have sufficed for standing.

First, the court was skeptical of the plaintiffs' allegation that they never would have spent money at Neiman Marcus had they known of its alleged cybersecurity lapses, and that Neiman Marcus therefore was unjustly enriched. The court noted that prior cases recognizing similar injuries involved the purchase of defective products, an allegation absent in this case.

Second, the court declined to confer standing based on the plaintiffs' claim that they had lost control over the value of their personal information. The court noted that such a claim presupposes there is a federal property right in personal information, but that currently there is no federal law conferring such a property right.

Court Rejected Neiman Marcus' Argument on Causation and Redressability

The Seventh Circuit rejected Neiman Marcus' argument that the plaintiffs failed to allege causation and redressability. With respect to causation, Neiman Marcus had argued that the plaintiffs had not shown that their injuries were traceable to its data breach rather than to one of several other large-scale breaches that took place around the same time. The court held that the plaintiffs had pled sufficient facts to shift the burden to defendants to show which retailer was responsible.

Finally, the court rejected Neiman Marcus' arguments that the plaintiffs' injuries are not redressable by a judicial decision because they already have been reimbursed for fraudulent charges by their credit card companies. The court held that the "zero liability" feature Neiman Marcus relied upon could vary by credit card company or exclude customers who used debit cards. Accordingly, the court held that the plaintiffs alleged injury-in-fact, causation and redressability sufficient to establish Article III standing.

Where Does *Remijas* Fit in the Landscape of Data Breach Cases?

Remijas is the first federal appellate court decision addressing the Supreme Court's holding in *Clapper* suggesting that future injury must be "certainly impending" to satisfy Article III standing. In holding that members of the proposed *Remijas* class who had not suffered any actual theft or fraud had nevertheless adequately alleged standing, the Seventh Circuit sided with district courts in the Ninth Circuit that have found risk of future identify theft or fraud sufficient to confer standing even where there is no evidence of fraudulent use of that information. But, as discussed below, many district courts have found such alleged harm too speculative to establish Article III standing. Given these divergent rulings, it is worthwhile to pause and examine the landscape in the emerging area of the law.

For standing purposes, data breach cases can be viewed as falling into one or more of three categories:

- **Category 1:** claims of unauthorized access to a database exposing private consumer or health information to the intruder but with no evidence that the private information was copied or stolen and no evidence of misuse of such information;
- **Category 2:** claims of unauthorized access and exposure paired with evidence the private information was stolen, but with no evidence of any fraudulent or other misuse; and
- **Category 3**: claims of unauthorized access to the defendant's database plus evidence that private information was stolen combined with evidence of fraudulent use (such as fraudulent charges on a credit card).

Courts consistently hold that plaintiffs in Category 1 cases lack Article III standing.[3] Several courts, most notably district courts in the Ninth Circuit and the Seventh Circuit in *Remijas*, have held that claims of potential future identity theft or fraud in Category 2 cases are sufficient to confer standing.[4] However, other district courts have held that Category 2-type future injury claims are too speculative to establish standing.[5] Outside the Ninth Circuit and prior to *Remijas,* several courts rejected even Category 3-type standing claims, usually on the ground that the alleged loss (*e.g.*, fraudulent credit card charges) had been reimbursed.[6]

The question raised by *Remijas* is whether the Seventh Circuit's ruling will begin a shift in the courts toward more liberal standards for the pleading of Article III standing, particularly in Category 2 cases. Barnes & Noble already has argued in its data breach class action pending in the Northern District of Illinois that the Seventh Circuit's ruling does not apply to the facts of that case, arguing the Seventh Circuit's decision was influenced by the allegation that 9,200 of the 350,000 stolen credit card numbers had been used in fraudulent charges. *Remijas* likely does not apply to the Barnes & Noble class action because it is a Category 1 case; the plaintiffs in the Barnes & Noble case alleged that hackers attempted to skim credit card information from pin pads utilized in Barnes & Noble stores but have been unable to allege that class representatives' information actually was stolen.

Practice Points

Given the ubiquitous nature of the Category 2- and 3-type injuries alleged by the plaintiffs in Remijas, the Seventh Circuit's ruling may limit the ability of defendants to use the Article III standing defense in the Seventh Circuit. Whether other circuits follow suit will be watched closely by both the plaintiffs' bar and companies that handle consumer financial information. Furthermore, although offering fraud protection following a data breach is required by law in at least Connecticut,[7] companies that are not required to do so (*i.e.*, because the impacted individuals are not from states requiring such protection) should more carefully evaluate whether offering such protection to customers may be seen by a court as a concession that the risk of fraud or identity theft is substantial.

Return to Table of Contents

FCC Clarifies TCPA and Expands the Scope of Potential Liability

The FCC issued a declaratory ruling and order indicating that it will interpret the TCPA in a manner that will make it more difficult for businesses to reach out to consumers by phone without prior express consent, raising the potential for significant new liabilities.

On July 10, 2015, the Federal Communications Commission (FCC) issued a declaratory ruling and order revising its regulations implementing the Telephone Consumer Protection Act (TCPA). The newly revised regulations become effective

[3] There have been a number of decisions rejecting standing in this area, including: *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (holding that plaintiffs' "allegations of an increased risk of identity theft resulting from a [data] security breach are insufficient to secure standing" where it was "not known whether the hacker read, copied, or understood the data"), and *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015) (holding the breach of a health care service's network exposing employees' personal data did not constitute Article III standing absent concrete allegations of fraud or misuse).

[4] For example, see *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916 (holding that the "risk Plaintiff's personal data will be misused by the hackers who breached Adobe's network is immediate and very real"), and *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,* 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014) (holding that plaintiffs' allegations that their personal data was collected by Sony and then wrongfully disclosed was sufficient to establish Article III standing).

[5] For example, see *In re Zappos.com, Inc.,* No. 3:12-CV-00325-RCJ-VP, 2015 WL 3466943, at *7-8 (D. Nev. June 1, 2015) (threat of future harm to 24 million Zappos customers from January 2012 data breach not sufficiently immediate to confer standing where none of the 12 name plaintiffs had pled any credit card fraud or identity theft in years following breach), and *Galaria v. Nationwide Mut. Ins. Co.,* 998 F. Supp. 2d 646, 650 (S.D. Ohio 2014) (holding the theft and subsequent dissemination of personal information did not merit Article III standing).

[6] For example, see *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, No. CIV.A. 13-7418 CCC, 2015 WL 1472483 (D.N.J. Mar. 31, 2015) (holding the fraudulent filing of a plaintiff's tax return did not constitute actual injury because they had been reimbursed); and *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014) (finding that there was no Article III standing because plaintiffs failed to show that unauthorized charges to six out of 33 of their cards directly linked to the data breach itself). For a contrary example, see *Moyer v. Michaels Stores, Inc.,* No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014) (holding that plaintiffs faced credible, nonspeculative risk of future harm by, in part, pointing to fraudulent charges incurred within two weeks of shopping at Michaels, noting "the chain of causation connecting a data security breach and identity theft is not so attenuated that it makes the latter risk speculative or hypothetical").

[7] There is some disagreement as to whether California imposes such a requirement. Some read the California law to require 12 months of identity theft protection while others read the statute to say that if identity theft protection is offered, it must be for 12 months. We discussed the California law in greater detail in our October 2014 Privacy & Cybersecurity Update. For more information on the Connecticut requirement, see our June 2015 Privacy & Cybersecurity Update.

immediately and respond to a number of requests for further FCC guidance on TCPA matters. Recent TCPA cases have led to substantial awards to plaintiffs, and the order can be expected to expand the scope of potential liability under the statute.

The TCPA limits the ability of businesses and telemarketers to make certain calls to consumers' wireline and wireless phone numbers without receiving prior express consent, and provides both for FCC enforcement of TCPA rules and a private right of action. Among other key points, the declaratory ruling and order:

- **Clarified and Broadened the Definition of an "Automatic Telephone Dialing System" (ATDS).** The TCPA defines an ATDS as "equipment which has the capacity (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers." The FCC clarified that "capacity" includes present and potential future capability of the dialing equipment and that a case-by-case determination is necessary to determine if equipment that requires human intervention is covered.
- **Reiterated or Expanded the Covered Set of "Calls" Under the TCPA.** The FCC confirmed its long-held view that text messages are "calls" covered by the TCPA, while also holding that Internet-to-phone text messages require consumer consent under the TCPA.
- **Expanded the Means by Which Consumers Can Revoke Their Previously Given Consent.** The FCC clarified that under the TCPA, the caller has the ultimate burden to demonstrate prior express consent of the called party, that the called party may revoke consent at any time and through any reasonable means, and callers may not limit the manner in which revocation may occur.
- **Established a One Call "Safe Harbor" Rule for Reassigned Numbers.** The order clarified that "called party" means "the subscriber, *i.e.*, the consumer assigned the telephone number dialed and billed for the call, or the non-subscriber customary user of a telephone number included in a family or business calling plan." As a result, callers now may incur TCPA liability for reassigned phone numbers, although the FCC did establish a one-call safe harbor, finding that after the first post-reassignment call to a number, the caller should be considered to have constructive knowledge of the reassignment. The order also touched on several other TCPA issues that have recently been the subject of petitions before the FCC, including but not limited to the appropriate use of exceptions for time-sensitive calls, the use of one-time text coupons and the use of call-blocking technologies.

Possible Impact of Declaratory Ruling and Order

The declaratory ruling and order is intended to "affirm the vital consumer protections of the TCPA while at the same time encouraging pro-consumer uses of modern calling technology." Given the successful use of the TCPA as a basis for class actions in recent years — Capital One and three collection agencies earlier this year settled a TCPA class action lawsuit for $75 million — any FCC statement expanding the statute's scope also can be expected to set off a new round of litigation.

Return to Table of Contents

State AGs Urge Congress to Preserve State Authority to Respond to Data Breaches

State and territorial attorneys general have urged Congress not to pre-empt existing state laws on data breaches, arguing that states have an important enforcement role to play when protecting consumers.

On July 7, 2015, 47 state and territorial attorneys general sent a letter to congressional leaders urging them not to pre-empt state data security and breach notification laws in a proposed federal data security and breach notification bill.[8] Although the status of the issue remains unsettled, a variety of current federal data breach notification bills provide for such pre-emption. The attorneys general letter argues that states pay a critical front-line role in protecting consumers against misuse and theft of their data, and that federal pre-emption would undermine that important function.

Existing State Role

States have so far taken the lead in implementing laws relating to data breach disclosure, with California passing the first data breach notification law in 2003. To date, 47 states have passed some form of data breach notification law. In their letter to congressional leaders, the state attorneys general note that they have played a critical role in protecting consumers against identity theft and improper data security practices. As an example of the importance of their role, the attorneys general claim that Illinois' data breach notification law has enabled the Office of the Illinois Attorney General to help over 38,000 Illinois residents remove more than $27 million in unauthorized charges from their accounts. Many of those breaches, the attorneys general argue, would have been too small to raise concerns at the federal level but had a significant impact at the regional and local level.

The attorneys general also point out that states can and do amend their laws to adapt to changing practices and issues. As

[8] Letter from the National Association of Attorneys General (NAAG) to congressional leaders (July 7, 2015), *available at* http://www.naag.org/assets/redesign/files/sign-on-letter/Final%20NAAG%20Data%20Breach%20Notification%20Letter.pdf.

consumers become concerned about the collection and storage of new types of sensitive information, such as biometric data, some states have sought to amend their laws to address these issues.

Call for Federal Standards

Businesses that operate in multiple jurisdictions have complained about the differing standards for data breach notifications and data protection among the myriad state laws within the United States, and have called for uniform federal legislation to address this issue. A number of different bills have been introduced in Congress to provide for such a uniform standard, many of which provide for pre-emption of conflicting state laws.

For example, the proposed Data Security and Breach Notification Act of 2015 would pre-empt state data breach notification and data security laws.[9] The proposed act, much like data security and breach notification laws enacted by the states, requires covered entities to maintain reasonable security measures appropriate for the size and complexity of the entity and to notify individuals affected by a data breach. The most recent draft empowers the FTC to enforce violations of both the data security and breach notification sections of the bill and permits state attorneys general, as *parens patriae*, to bring civil actions on behalf of residents of their state to enjoin further violations, compel compliance and obtain civil penalties. Despite this complementary enforcement power, however, the proposed act would prohibit states from enacting their own legislation in this area. It is this type of pre-emption that has triggered the attorneys general to write to Congress to argue against such a measure.

Next Steps

Although companies subject to differing state laws have called for federal pre-emption, the attorneys general have united to oppose such a step. Companies subject to state data security and data breach notification laws should monitor the status of the various proposed data security and breach notification bills to understand how their obligations would change under a uniform federal data security and breach notification regime.

Return to Table of Contents

[9] Whether the federal bill will ultimately pre-empt state data security and breach notification laws remains unclear. The most recent discussion draft includes a note stating that the "parties of this staff draft have not yet reached agreement on the scope of preemption and continue to discuss this issue." Data Security and Breach Notification Act, H.R. ___, 114th Cong. § 6(a) (2015), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/analysis/20150312DataSecurityDraft.pdf.

Lloyd's Report on Cyberattack Highlights Potential Harm and Insurance Issues

Lloyd's of London has released a report outlining the impact of a particular type of cyberattack on the U.S. energy infrastructure and the limited recovery available in today's insurance market.

In early July 2015, insurance market Lloyd's of London released a co-written report predicting that a major cyberattack on the East Coast of the United States could trigger up to $1 trillion in damages, roughly $71 billion of which would be covered by insurance. Although focused on the impact of such an attack and how its effects would propagate through the economy, the report provides some important lessons about the state of cyberinsurance in today's market.

A Hypothetical Scenario

The report, titled "Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid,"[10] posits an attack focused on a particular vulnerability affecting power generators known as the "Aurora vulnerability." In 2007, the Idaho National Laboratory's Aurora Project demonstrated that this particular vulnerability could allow attackers to damage generators by opening and closing certain circuit breakers remotely. According to the report, even if only 10 percent of such attacks were successful, the result could leave 93 million people across 15 states without power.

Such a widespread blackout would be disastrous. The report predicts a rise in mortality rates as various health and safety systems fail, a decline in trade as ports shut down and the transportation infrastructure is hobbled, and disruption to water supplies as electric pumps remain inoperable. The report projects that such losses could range from $243 million up to $1 trillion in the most extreme scenario. The range of policyholders that would suffer such losses would include individuals, power generation companies, companies that lose power and homeowners.

Insurance Issues

In the report, Lloyd's estimates that, with losses ranging from $243 million to $1 trillion, insurers could expect to pay $21.4 billion to $71 billion in claims. The losses described in the report could implicate both traditional and cyber-specific policies. Recovery under cyber-specific policies may be available to power generation companies, for example, as they would be

[10] The report is *available at:* https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

directly affected by the cyberattack. Other companies — such as food distribution companies that would suffer losses due to spoiled goods — likely would seek to recover damages under their more traditional policies. The types of claims under the various policies could vary widely, as could policyholders' ability to recover based on the specific requirements and exclusions under their policies.

Some observers have noted that the Lloyd's report demonstrates that — contrary to some expectations — it is possible for insurance companies to model the risks of a cyberattack. The report itself notes that responding to the challenges posed by a cyberattack will require innovation on the part of insurance companies — some of which will be driven by the industry's ability to reduce some of the uncertainties that exist around cyberattack exposure. Lloyd's argues that the industry could be able to reduce some of these uncertainties through increased sharing of cyber risk data.

Key Takeaways

The Lloyd's report provides a stark reminder of the potential harm arising from a cyberattack on the U.S. infrastructure, and the challenges insurers and insureds alike would face in trying to model the financial risk and recover damages. As the threats and the industry's understanding of the related risks evolve, and as more and more companies adopt measures to reduce the risks of cyberattacks, the availability, cost and limitations of cyber-specific and other insurance is likely to change.

Return to Table of Contents

FTC Launches 'Start With Security' Initiative: Releases Data Security Guidance and Announces Nationwide Conference Series

The FTC has launched a new initiative to provide guidance on data security practices. The initiative consolidates lessons learned through multiple FTC data security cases and is intended to help businesses avoid FTC scrutiny in the future.

On June 30, 2015, the Federal Trade Commission (FTC) announced its new "Start With Security" initiative that includes guidance for businesses on data security practices as well as a nationwide series of conferences aimed at small- to medium-sized businesses. The information shared through the guidance and conferences, say the FTC, are based on the cases the FTC has brought to date and are intended to help businesses avoid FTC scrutiny in the future.

Start With Security Guidance

As part of Start With Security, the FTC released a document of the same name that provides 10 lessons that companies should learn about data vulnerabilities and how to reduce the risks they pose.[11] For each lesson, the FTC also shared related practical advice and specific examples of companies that were subject to FTC legal action based on similar vulnerabilities or actions.

The lessons the FTC shared are the following:

1. **Start With Security.** Factor data security into the decision-making in every department of the business. Companies should not collect information that is not needed and should hold on to it only as long as the company has a legitimate need to do so. Furthermore, companies should not use sensitive information when it is not necessary to do so, such as in employee training sessions or in creating testing or development environments.
2. **Control Access to Data Sensibly.** When a company does have sensitive information, put limits on who can access it. Not everyone needs unrestricted access to the entire network and all the information in it. Companies also should be careful in granting administrative-level access to their systems so that only a select group of people can view and alter sensitive information. For paper files, companies can implement access controls through simple measures such as placing the files in a locked file cabinet and controlling who has access to the key.
3. **Require Secure Passwords and Authentication.** Companies should require strong password practices among their employees. They should not allow dictionary words as passwords or the use of the same password across multiple systems. Companies should store passwords securely — even the strongest password is rendered ineffective if the password itself is stored in cleartext. In addition, companies should implement controls to protect against brute-force password attacks and should be mindful of back doors and other tricks that can be used to bypass password authentication.
4. **Store Sensitive Personal Information Securely and Protect It During Transmission.** Companies should seek to protect sensitive information throughout its life cycle, including when that information is transmitted to others, downloaded to a laptop or other device, or destroyed. Companies also should make sure that those with access to the information are properly trained in the methods being used to secure it. In developing secure storage, transmission and destruction techniques, companies should use industry-tested and accepted methods rather than seek to create their own.

[11] The Start With Security guidance is available at: https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

5. **Segment Your Network and Monitor Who's Trying to Get In and Out.** Companies should use tools such as firewalls to segment their networks and limit access between devices on the network and between the network and the Internet. Companies also should implement intrusion detection and prevention tools to monitor their networks and identify malicious activities. Without proper network segmentation, an attacker that gains access to a less-protected part of the network can use that as a gateway into more sensitive areas.
6. **Secure Remote Access to Your Network.** When designing their network security procedures, companies should be sure to take into account remote users and the steps they can take to secure those connections. Before allowing vendors to access their systems, companies should verify those vendors' security practices, including how they store the credentials used to access the companies' systems. Similarly, companies should ensure that employees with remote access rights have in place antivirus and firewall protections. Finally, similar to Lesson 2 above, when allowing remote access to vendors or employees, companies should have controls in place to limit that access to the information and resources that are necessary.
7. **Apply Sound Security Practices When Developing New Products.** Companies should keep security practices and issues in mind when developing new products. They should consider how users are likely to use the product, what kind of information the product may gather — even inadvertently — and how that information is stored and transmitted. Development engineers should be trained in secure coding practices, and companies should consider the security risks posed by any third-party tools incorporated into their products. When developing applications for existing platforms, companies should heed the advice of the platform experts and obey any secure development guidelines for that platform. Companies also should test and retest their products for security issues, particularly any product features that are advertised as providing privacy and security protections. Finally, companies should test for common vulnerabilities in their products. The security community frequently reports on well-known exploits in products, and companies should be aware of these reports and test their products for these vulnerabilities.
8. **Make Sure Your Service Providers Implement Reasonable Security Measures.** Companies' security protection obligations include the vendors to whom they provide sensitive information. Companies should take reasonable steps to select providers that are able to implement appropriate security measures, include their security requirements in their contracts and monitor providers for compliance.
9. **Put Procedures in Place to Keep Your Security Current and Address Vulnerabilities That May Arise.** Security is not a one-time analysis, and companies should be sure to apply security updates to third-party products on their networks and in their products and constantly monitor for new vulnerabilities and exploits to existing products.
10. **Secure Paper, Physical Media and Devices.** Network and application security is not the end of the analysis, and many of the same lessons apply to paperwork and physical media like hard drives, laptops, flash drives and disks. Companies should securely store and control access to paper files and devices that are used to collect sensitive information (such as point of sale devices or ATM machines) and should be mindful of how physical devices that store sensitive information are moved and transported. Back-up tapes or laptops containing sensitive information are vulnerable to theft or loss, and sensitive information could be released as a result. Finally, companies should be careful to securely dispose of sensitive information. Secure destruction includes shredding of paper documents and using available technologies to securely wipe the contents of hard drives or other media that may hold sensitive information.

Announcement of Start With Security Conferences

Simultaneously with its release of the Start With Security guidelines described above, the FTC announced a series of conferences across the country to discuss security practices. These conferences are aimed at small- to medium-sized businesses, and the FTC has said that it will provide practical tips and strategies for implementing effective data security measures.

The first conference is scheduled for September 9, 2015, at the University of California Hastings College of the Law in San Francisco and is aimed at startups and developers. The second will take place in Austin, Texas on November 5, 2015.

Key Takeaways

The FTC's Start With Security initiative likely will be an important factor in future FTC actions, and businesses that do not heed the lessons will be at risk of FTC scrutiny. By design, the lessons and guidance explained in the FTC's Start With Security report are not new; they reflect the FTC's experience over the course of over 50 investigations undertaken by the FTC in the data security area, as well as the various reports the FTC has issued in recent years. What is new is the aggregation and consolidation of the FTC's experience and policy guidance into a single document. Some companies — in particular those fighting FTC enforcement actions — have complained that the FTC's piece meal enforcement actions and policy documents have not provided the community with a clear understanding of what security measures they should be taking in order to prevent FTC action. By consolidating this information into a single source, the FTC has sought to address that concern and, in doing so, may have strengthened its case against future companies.

Return to Table of Contents

FFIEC Releases Voluntary Cybersecurity Assessment Tool

The FFIEC has issued a voluntary Cybersecurity Assessment Tool to help institutions assess their cybersecurity exposures and processes for addressing known risks.

On June 30, 2015, the Federal Financial Institutions Examination Council (FFIEC) released a voluntary Cybersecurity Assessment Tool to assist financial institutions in evaluating their cybersecurity risks and preparedness and determining whether their existing cybersecurity controls and practices are aligned with their inherent risk profile.[12]

Background

The assessment tool is the product of the FFIEC's 2014 pilot assessment of cybersecurity preparedness at more than 500 community financial institutions, which found significant variances in inherent risks across the institutions. Following the pilot assessment, the FFIEC identified several cybersecurity action items, including creating the assessment tool, improving incident analysis, crisis management, training, policy development, and collaboration with law enforcement and intelligence agencies.

Cybersecurity Assessment Tool

The assessment tool is a methodology for conducting a self-assessment of an institution's cyber risk. Financial institutions are provided with a matrix and instructed to evaluate which description of the organization best matches the institution's cybersecurity risk and preparedness across various categories. The tool consists of two parts — Inherent Risk Profile and Cybersecurity Maturity — and is ultimately designed to help senior management determine whether the institution's level of cybersecurity preparedness is appropriate given its internal risk profile. The user guide provides targeted guidance for senior management and the board of directors, emphasizing the goal of making cybersecurity an executive-level responsibility rather than just an IT function.

The first part of the assessment, the Inherent Risk Profile, considers the institution-specific cybersecurity risks across five categories, for which the user guide provides the following descriptions:

1. **Technologies and Connection Types.** Certain types of connections and technologies may pose a higher inherent risk depending on the complexity and maturity, type of connections and nature of the specific technology products or services. This category includes number of Internet service provider and third-party connections, whether systems are hosted internally or outsourced, number of unsecured connections, use of wireless access, volume of network devices, use of end-of-life systems, extent of cloud services and use of personal devices.
2. **Delivery Channels.** Various delivery channels for products and services may pose a higher inherent risk depending on the nature of the specific product or service offered. Inherent risk increases as the variety and number of delivery channels increases. This category addresses whether products and services are available through online and mobile delivery channels and the extent of ATM operations.
3. **Online/Mobile Products and Technology Services.** Different products and technology services offered by institutions may pose a higher inherent risk depending on the nature of the specific product or service offered. This category includes various payment services, such as debit and credit cards, person-to-person payments, merchant remote deposit capture, treasury services and clients and trust services, global remittances, correspondent banking, and merchant-acquiring activities. This category also includes consideration of whether the institution provides technology services to other organizations.
4. **Organizational Characteristics.** This category considers organizational characteristics, such as mergers and acquisitions, number of direct employees and cybersecurity contractors, changes in security staffing, number of users with privileged access, changes in IT environment, locations of business presence, and locations of operations and data centers.
5. **External Threats.** The volume and type of attacks (attempted or successful) affect an institution's inherent risk exposure. This category considers the volume and sophistication of the attacks targeting the institution.

Institutions should use these criteria to rate their risk level for each category as: least, minimal, moderate, significant or most, without considering any mitigating controls the institution may have in place.

The second part of the assessment, Cybersecurity Maturity, evaluates the existing cybersecurity controls and practices of the institution across five domains, ranking each as: baseline, evolving, intermediate, advanced or innovative. The FFIEC notes that the baseline level of cybersecurity maturity is consistent with legally required minimum risk management and control expectations. Each category provides several assessment factors and subfactors to guide this analysis. The user guide provides the following descriptions:

[12] The Cybersecurity Assessment Tool is available at: http://www.ffiec.gov/cybersecurity.htm.

1. **Cyber Risk Management and Oversight.** Addresses the board of directors' oversight and management's development and implementation of an effective enterprisewide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.
   - *Assessment factors:* governance, risk management, resources, and training and culture.
2. **Threat Intelligence and Collaboration.** Includes processes to effectively discover, analyze and understand cyber threats, with the capability to share information internally and with appropriate third parties.
   - *Assessment factors:* threat intelligence, monitoring and analyzing, and information sharing.
3. **Cybersecurity Controls.** The practices and processes used to protect assets, infrastructure and information by strengthening the institution's defensive posture through continuous, automated protection and monitoring.
   - *Assessment factors:* preventative controls, detective controls and corrective controls.
4. **External Dependency Management.** Involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the institution's technology assets and information.
   - *Assessment factors:* connections and relationship management.
5. **Cyber Incident Management and Resilience.** Includes establishing, identifying and analyzing cyber events; prioritizing the institution's containment or mitigation; and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber incident.
   - *Assessment factors:* incident resilience planning and strategy; detection, response, and mitigation; escalation and reporting.

Institutions should analyze the results of the two portions and use them as a guide to determine whether the institution's inherent risk profile is aligned with its level of cybersecurity maturity across the various categories. (See summary table below.) In the event that the two are not aligned, the institution should adapt its practices so as to better inform its risk management strategy. Institutions should repeat the analysis over time to provide continuing guidance as to cybersecurity preparedness.

Conclusion

The FFIEC will periodically update the assessment tool as the cybersecurity landscape and threats evolve, particularly with respect to minimizing the burden for financial institutions with low cybersecurity risk profiles. Additionally, financial institutions are encouraged to comment on the assessment tool, pursuant to a forthcoming notice in the Federal Register. The FFIEC also provides various additional resources on the FFIEC website to assist institutions in improving their cybersecurity.[13]

While the assessment tool is currently voluntary, the Office of the Comptroller of the Currency and the Federal Reserve Board have announced plans to incorporate the tool into their examination process for evaluating the safety and soundness of financial institutions by late 2015 or early 2016.

[13] The user guide is available at: https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_User_Guide_June_2015_PDF2_a.pdf. Additional resources are available at: http://www.ffiec.gov/cybersecurity.htm.

Cybersecurity Assessment Tool Summary

Part I: Inherent Risk Profile Least, Minimal, Moderate, Significant, Most	**Part II: Cybersecurity Maturity** Baseline, Evolving, Intermediate, Advanced, Innovative
Technologies & Connection Types	Cyber Risk Management & Oversight
Delivery Channels	Threat Intelligence & Collaboration
Online/Mobile Products & Technology Services	Cybersecurity Controls
Organizational Characteristics	External Dependency Management
External Threats	Cyber Incident Management & Resilience

Source: Federal Financial Institutions Examination Council

Return to Table of Contents

Rhode Island Revises Personal Data and Identity Theft Prevention Laws

Rhode Island has updated its data protection laws in ways that reflect growing trends in such laws. The new laws include a specific deadline for notifying consumers of data breaches and an expansion of the scope of the state's data protection requirements.

On June 26, 2015, Rhode Island updated its existing data protection laws to, among other things, include a specific deadline for notifying consumers of data breaches and expand the scope of data protection requirements. The new law replaces the state's existing data protection laws, enacted in 2005, and reflects certain growing trends in state data protection laws.

Overview of New Requirements

Rhode Island's new data protection law[14] makes a number of key changes to its existing laws, including:

- **Standard for Data Breach Notification.** Companies holding information on Rhode Island residents must notify those residents if there has been a data breach "which poses a risk of identity theft" to those residents.
- **Deadline for Data Breach Notification.** Companies must provide any required data breach notification with 45 days after discovery of the breach.
- **Notification of Attorney General and Credit Reporting Agencies.** In addition to notifying residents, if the breach affects more than 500 Rhode Island residents, companies also must notify the state attorney general and the major credit reporting agencies of the breach.
- **Information Security Program.** Companies must implement a "risk-based information security program" with reasonable security procedures and practices appropriate to the size and scope of the organization, the types of information collected and the purpose for which the information is collected.
- **Limits on Retention and Disposal Requirements.** Companies must retain information only for as long as necessary and must properly dispose of the information when it is no longer necessary.
- **Definition of Encryption.** Like many state statutes, the data breach notification obligation does not apply if the data was encrypted. Rhode Island's law, however, now includes a general definition of encryption to mean that the information is in a form where there is a "low probability of assigning meaning without the use of a confidential process or key."
- **Expansion of Information Protected.** The Rhode Island law now includes health information and information in paper form among the information protected.

Emerging Trends

Rhode Island's new law reflects a number of trends among state laws on data protection and privacy advocates. The state is the fifth to establish a precise deadline for notifying affected consumers. A number of states have specific deadlines when particular types of data have been accessed, such as health information, and a handful include specific deadlines for disclosure, with Florida having the shortest at 30 days. The requirements on secure data disposal, information security programs and the obligation to disclose a breach that simply poses a "risk of identity theft" reflect issues that have been gaining increased attention in the privacy community and are likely an indication of the direction other states may take with respect to their data protection laws.

Return to Table of Contents

[14] Identity Theft Protection Act, Senate Bill 0134, 2015 Reg. Sess. (R.I. 2015). The Act defines personal information as an individual's first name or first initial and last name with any of the following, when the name and data are not encrypted or are in hard copy paper format: Social Security number, driver's license number, Rhode Island identification card number, tribal identification number, account number or credit or debit number with any security or access code, medical or health insurance information, or email address with any security or access code.

Contacts in the Privacy and Cybersecurity Group

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Cyrus Amir-Mokri
Partner / New York
212.735.3279
cyrus.amir-mokri@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000

Return to Table of Contents