Skadden

PRIVACY & CYBERSECURITY UPDATE

NOVEMBER 28, 2014

CONTENTS (click on the titles below to view articles)

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 13, or your regular Skadden contact.

EU ISSUES GUIDELINES ON 'RIGHT TO BE FORGOTTEN'

In a landmark May 2014 decision, Europe's top court, the Court of Justice of the European Union, established a "right to be forgotten."[1] In *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12)*, the court held that, upon the request of a European citizen, search engines have an obligation to "de-list" search results that link to information about the requesting individual if the information is inaccurate, outdated or irrelevant. While search engines can deny the request where there is an overriding public interest in the information, the clear message from the court was that an individual's privacy rights would trump in most cases. Google has reported that since it put procedures in place to comply with the court's ruling, it has received approximately 175,000 de-listing requests and agreed to de-list approximately 60 percent of the time.[2]

While the "right to be forgotten" rule was broad in scope, its jurisdictional reach was limited to the country in which the request was made. For example, if a French citizen submitted a takedown request in France, a search engine only had to take down the search results for the search engine dedicated to that country (such as Google.fr). Thus, the results still would be accessible on the main search engine site (*e.g.*, google.com) or on the dedicated search sites of other European countries. Europe's Article 29 Working Party, the EU group composed of the data privacy commissioners from individual Member States, is now seeking to change that reality.

On November 26, the Working Party issued new guidelines (Guidelines) relating to the "right to be forgotten" that would require search engines to remove de-listed links on all of their domains.[3] In the view of the Working Party, without such a broad application, the "right to be forgotten" mandate too easily could be circumvented.

The Guidelines also critique the practice (used by Google) of posting a notice when parts of a search result have been de-listed. According to the Working Party, there is no legal requirement to do so, and in fact such information should not be made public. The effect of this Guideline is that search engines must either not include such a notice or include it every time a user searches for a name, whether de-listing took place or not. Similarly, the Working Party critiqued the practice of search engines informing websites that certain search results that would normally point to their sites have been delisted. According to the Guidelines, there is no legal basis to support such regular contacts.

In addition, the Guidelines state that search engines must allow multiple means for individuals to contact the search engine to request de-listing, rather than requiring them to follow a method specified by the search engine. This appears to be clearly directed at Google, which has set up an online form for users to complete if they want a search result to be de-listed.

When a search provider refuses a de-listing request, the Guidelines state that the company should provide "sufficient explanation" to the data subject about the reasons

[1] See our May *Privacy & Cybersecurity Update* for a more complete description of that decision.
[2] Although the European Court of Justice ruling and the new Guidelines apply to all search engines, Google has been most often linked to this development, because of Google's status as the search engine of choice in the EU.
[3] The Guidelines may be found at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

for the denial and inform the individual that he or she can appeal to the applicable Data Protection Authority (DPA) or to court.

The Guidelines also set some limitations on the application of the "right to be forgotten" rule. For example, they acknowledge that, as a rule, the right to de-listing should not apply to search engines with a restricted field of action, particularly in the case of search tools of websites of newspapers.

Finally, the Working Party tacitly acknowledged the backlash resulting from the *Gonzalez* opinion. Many argued that the European Court of Justice's decision throttled free speech in the name of individual privacy. The Guidelines include a number of statements that seek to assuage those concerns. For example, the Guidelines stress the importance of balancing the public interest with de-listing requests and that the impact on freedom of expression should "prove to be very limited." According to the Working Party, the public interest will be greatest where the data subject plays a role in public life, and the Guidelines include criteria for determining whether someone is a public figure. Perhaps even more importantly, the Guidelines concede that, in some cases, a private individual's life may have aspects that are of public interest and therefore not subject to de-listing.

Although the Guidelines are not firmly binding, the views of the Working Party always have held great sway in the privacy debate in the EU. While the Guidelines' impact on search engines remains to be seen, one thing is clear: The debate over the right to be forgotten will continue.

Return to Table of Contents

FFIEC OBSERVATIONS ON BANK CYBERSECURITY PROVIDES IMPORTANT GUIDELINES FOR EVERY INDUSTRY

As we reported in our June *Privacy & Cybersecurity Update*, during the summer of 2014 the Federal Financial Institutions Examination Council (FFIEC) conducted a cybersecurity assessment at approximately 500 community banks in order to assess and evaluate their level of preparedness to respond to, and mitigate, cyber-attacks.[4]

On November 3, 2014, the FFIEC issued a General Observations document, which summarized its insights from that assessment, as well as a short Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement (FFIEC Statement), which set forth several recommendations. The General Observations document is available here and the FFIEC Statement here.

Although the FFIEC's observations resulted from its assessment of community banks, the suggestions it makes, including the questions it proposes asking, provide a solid blueprint for any company in any industry to consider when evaluating its cybersecurity preparedness.

FFIEC STATEMENT ENCOURAGES PARTICIPATION IN FS-ISAC

The FFIEC Statement recommends that all financial institutions participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC, which was launched in 1999, is a member-owned resource of the financial services industry. It is used for sharing the analysis of cyber- and physical-threat intelligence. Membership in FS-ISAC is already recommended by the Department of the Treasury, the Office of the Comptroller of the Currency (OCC), the Department of Homeland Security and the U.S. Secret Service. Both the U.S. Treasury and DHS rely on the FS-ISAC to disseminate critical information to the financial services sector. The FFIEC stresses that information sharing is a critical tool in identifying,

[4] The FFIEC is an interagency body empowered to prescribe uniform principles and standards for the Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC) and Consumer Financial Protection Bureau (CFPB).

responding to and mitigating cybersecurity threats and incidents, especially in an industry like financial services, in which a single institution's vulnerabilities can expose the entire sector.

In encouraging participation in the FS-ISAC, the FFIEC highlights two points that financial institutions, and indeed C-suite executives in every organization, should remember: (i) "Management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly," and (ii) Management needs to establish policies and procedures that will allow them to evaluate and act upon the growing amount of cyber threat and vulnerability information they are receiving.

FFIEC GENERAL OBSERVATIONS

The FFIEC also issued general observations resulting from its assessment, noting that these observations should not be construed as formal "guidance." Nonetheless, the observations provide a roadmap as to how the FFIEC views this critical issue. We summarize these observations below. In addition, the FFIEC provided a check list of "Questions to Consider" that all organizations can use. We have reproduced these questions at the end.

- The amount of risk an institution faces must be assessed by looking at the type, volume and complexity of operational considerations, such as connection types (*e.g.*, wireless networks, bring-your-own-device (BYOD) policies, LANs that connect to other networks and virtual private networks), products and services offered (as different financial products and services create different cyber risks), and technologies used. Such risk should be analyzed independently of whatever risk-mitigation steps the company has implemented. For example, the type and amount of connections an institution has can expose it to increased threats. Similarly, an entity that relies on Web services to offer its products is more susceptible to denial-of-service attacks.
- In many cases, boards discuss cybersecurity with management only when an industry cyberattack has been widely reported or the financial institution itself experiences an attack. The FFIEC observed that discussing cybersecurity issues in regular board and senior management meetings, even when there is no imminent issue, will help financial institutions "set the tone from the top and build a security culture." This includes clearly defining roles and responsibilities to identify, assess and manage cybersecurity risks. In addition, regular cybersecurity training at all levels is critical since employees are any institution's "first line of defense."
- Organizations rely too heavily on media reports and third-party service providers to gather information on cybersecurity threats, given that management is expected to monitor and maintain sufficient awareness of cybersecurity threats. The FFIEC therefore strongly encourages participation in information-sharing forums such as FI-SAC.
- Financial institutions should have points of contact with local or federal law enforcement so that they can respond efficiently to threats before they manifest and to incidents once they occur.
- Financial institutions maintain event logs so they can understand a cyber incident *after* it occurs. While this is useful, organizations should monitor event logs on an ongoing basis for anomalies and analyze those anomalies with information from other sources. Such actions will improve reports to management and the board.
- When financial institutions change their information technology environment, they should ensure they are also reviewing and updating their control to prevent unauthorized access to their systems.
- While financial institutions generally encrypt customer information in transit, they also should consider encrypting sensitive data such as proprietary and important technical information.

- Financial institutions should routinely scan IT networks for vulnerabilities and anomalous activity, test systems for their potential exposure to cyber-attacks and remediate issues when identified.
- Given that the IT systems of many financial institutions are interconnected, management should review the corrective controls in place at third parties with whom they interconnect, in order to gain more complete views of their own risks.
- Before executing contracts with a third party, management should consider the risks of the third party's cybersecurity controls and understand its incident response plans.
- Financial institutions should have procedures for notifying customers, regulators and law enforcement when a cyber-attack involves personally identifiable customer information.
- Financial institutions also should document their procedures for incident detection and response, and have procedures to support the timely escalation and decision-making in the event of cyber-attacks.
- Business continuity plans should cover cyber-attack incidents, and the company should test these plans internally and with third parties.

QUESTIONS TO CONSIDER

Connections and Products and Services

- What types of connections does my financial institution have?
- How are we managing these connections in light of the rapidly evolving threat and vulnerability landscape?
- Do we need all of our connections? Would reducing the types and frequency of connections improve our risk management?
- How do we evaluate evolving cyber threats and vulnerabilities in our risk-assessment process for the technologies we use and the products and services we offer?
- How do our connections, products and services offered, and technologies used collectively affect our financial institution overall?

Gathering Threat Information

- What is the process to gather and analyze threat and vulnerability information from multiple sources?
- How do we leverage this information to improve risk management practices?
- What reports are provided to our board on cyber events and trends?
- Who is accountable for maintaining relationships with law enforcement?

Risk Management and Oversight

- What is the process for ensuring ongoing and routine discussions by the board and senior management about cyber threats and vulnerabilities to our financial institution?
- How is accountability determined for managing cyber risks across our financial institution? Does this include management's accountability for business decisions that may introduce new cyber risks?
- What is the process for ensuring ongoing employee awareness and effective response to cyber risks?

Cybersecurity Controls

- What is the process for determining and implementing preventive, detective and corrective controls on our financial institution's network?
- Does the process call for a review and update of controls when our financial institution changes its IT environment?
- What is our financial institution's process for classifying data and determining appropriate controls based on risk?
- What is our process for ensuring that risks identified through our detective controls are remediated?

External Dependencies

- How is our financial institution connecting to third parties and ensuring they are managing their cybersecurity controls?
- What are our third parties' responsibilities during a cyber-attack? How are these outlined in incident response plans?

Responding to Attacks

- In the event of a cyber-attack, how will our financial institution respond internally and with customers, third parties, regulators and law enforcement?
- How are cyber incident scenarios incorporated in our financial institution's business continuity and disaster recovery plans? Have these plans been tested?

PRACTICE POINTS

Although the FFIEC's observations resulted from its assessment of community banks, the suggestions it makes, including the questions it proposes asking, provide a solid blueprint for any company in any industry to consider when evaluating its cybersecurity preparedness. For example, the FFIEC correctly observes that many organizations only involve the board and senior management in cyber issues after an attack occurs or when there is an imminent threat. Involving the board and senior management at a much earlier stage to set the tone and establish a culture of security is even more critical. Similarly, evaluating a company's connections to third parties and such third parties' security controls is essential in an environment where hackers will seek vulnerabilities in a variety of ways, including third-party access points. Overall, the FFIEC observations demonstrate the common cyber risks that all companies face today.

Return to Table of Contents

REMARKS BY COMPTROLLER CURRY HIGHLIGHT OCC VIEWS ON CYBERSECURITY

On November 7, Comptroller of the Currency Thomas J. Curry made a number of important statements about cybersecurity protection for community banks and thrifts at the 10th Annual Community Bankers Symposium in Chicago. Comptroller Curry noted that while large institutions garner most of the press attention for data breaches, community banks and thrifts also suffer, as they must often compensate customers for fraudulent charges, replace credit and debit cards and monitor account activity for fraud, all of which entail significant costs. In Comptroller Curry's view, some of this expense should be borne by the merchants.

Comptroller Curry also acknowledged that smaller financial institutions, although facing many of the same cyber threats as larger banks, often lack the same internal resources to address this issue. He therefore encouraged community banks and thrifts to rely on resources such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), discussed earlier in this mailing, and on support from the Federal Financial Institutions Examination Council (FFIEC), which Comptroller Curry is chairman of.

Comptroller Curry highlighted the recent formation of the FFIEC Cybersecurity and Critical Infrastructure Working Group, which has issued a number of statements regarding cyber-attacks, as well as the FFIEC Cybersecurity Assessment, discussed earlier in this mailing. Significantly, Comptroller Curry stressed that the OCC expects management at every institution it supervises "to monitor and maintain sufficient awareness of cybersecurity threats and vulnerabilities." Comptroller Curry highlighted so-called "external dependency management," which entails focusing on interdependencies with third parties, evaluating how those connections might expose an institution to vulnerabilities, and establishing controls to mitigate those risks. This includes being aware of how employees may themselves expose the institution to risk by connecting to other devices or networks.

Comptroller Curry next turned his focus to third-party relationships and the potential cyber vulnerabilities they present to organizations, given that the third party in many cases has access to bank customers' personal information. The comptroller's attention to this issue is consistent with the OCC's general concern with third-party relationships. In October 2013, the OCC issued Risk Management Guidance on Third-Party Relationships that covered a wide range of issues related to selecting and relying on third-party providers. As Comptroller Curry noted, "Just because contractors have long client lists and hard-to-duplicate expertise doesn't mean they are infallible."

Comptroller Curry also cautioned that even if the OCC supervises a service provider because it is rendering critical services to multiple institutions, that supervision does not absolve a bank of its own need to determine and manage the risks of using the third-party service provider, taking into account the level of risk and complexity of the arrangement.

Return to Table of Contents

RETAILERS PETITION FOR FEDERAL DATA BREACH LAW

Since 2003, when California became the first state to enact a data breach notification law, a total of 47 states have enacted similar laws. Each of these laws require that owners of personal information notify individual residents of the applicable state when personal data has been compromised. Even though many of these state statutes are similar, there are sufficient differences and nuances to increase the cost of responding to data breaches. For example, the laws vary with respect to what type of breach triggers notification, the types of personal information and entities covered by the statute, the time frame for notification, and the form and content of the notification itself.

Although there has been talk for a number of years about the need for a single federal data breach law that would replace the patchwork of state laws that exist today, little progress has been made. However, the increase in large, national and highly publicized data breaches has sharpened the call for such a law. On November 6, 2014, industry representatives from the merchant and retail sector, ranging from the National Association of Convenience Stores to the Nebraska Retail Federation, sent a letter to Sens. Harry Reid and Mitch McConnell and Reps. John Boehner and Nancy Pelosi calling upon Congress to address the need for a uniform data breach notification law that is standardized across industries.

Rather than focus on the cost of responding to a data breach, the retailers sought to highlight the security risk of having different laws. The signatories highlighted their concern that different standards for different industries (such as financial services and health care) create security gaps that criminals can quickly exploit to the detriment of American consumers. For example, the letter notes that communications entities that transmit personal data and businesses handling that same data should be subject to the same notification and penalty schemes. Without such consistency, the signatories fear there will be inconsistent public notification and enforcement of the law. The letter concludes that all businesses, large and small, are vulnerable to a breach, and a standardized notification scheme would ensure that consumers receive the notification they deserve.

Even though Congress in 2014 drafted legislation addressing the issue, none of the bills have been passed. It remains to be seen if enough momentum will build within Congress to push through a standard data breach notification law.

Click here for a copy of the letter.

Return to Table of Contents

AUTOMAKERS ESTABLISH CONSUMER PRIVACY PROTECTION PRINCIPLES

On November 13, the Alliance of Automobile Manufacturers and the Association of Global Automakers, two leading trade associations for the United States' most prominent vehicle manufacturers, released Privacy Principles for Vehicle Technologies and Services (Principles) in a public commitment letter to the Federal Trade Commission (FTC).[5] The Principles, the first industrywide statement on the issue, directly address concerns that have been raised regarding the vast amounts of data that cars can collect without drivers being aware, including driving patterns and navigation data. The Principles establish a framework of baseline protections for consumer data generated by vehicle systems and require companies to receive permission for certain uses of data. As of now, 19 U.S. automakers — among them American Honda Motor Co., Ford Motor Company and General Motors LLC — have adopted the Principles.[6] Once committed, participating automakers (Participating Members) will implement the Principles by model year 2017 (which actually may begin as early as January 2016) at the latest, with a one-year extension available if engineering changes are necessary.

The adoption of the Principles highlights the growing focus on data collected through everyday devices — the so-called "Internet of Things." This action by the auto industry also is indicative of how industries are seeking to impose self-regulation on their members in an attempt to forestall the need for government privacy regulation.

THE SEVEN PRIVACY PRINCIPLES

In recent years, automakers have incorporated innovative technologies and services designed into vehicles to optimize vehicle performance and safety. Cars can, and do, collect enormous amounts of data through systems like General Motors' OnStar or built-in 4G data connections, generating information that is sent to manufacturers. As cars become "smarter," the data they can collect grows, including information about driver behavior and geographic location. The lack of regulations controlling the collection and use of such information led to calls for change, spurred by a 2014 U.S. Government Accountability Office (GAO) report concluding that the privacy policies of some providers of in-car location-based services were "unclear."[7] A number of states considered privacy laws that would regulate the industry. For example, California has considered legislation that would require automobile manufacturers to give vehicle owners far-ranging access to the data their vehicles collect.

The Principles represent an effort to address these concerns and stave off imposed regulation. Based on the FTC's Fair Information Practice Principles (FIPPs), the seven Principles address how Participating Members use, collect and share information linked or linkable to vehicles or their owners. Such information, designated "Covered Information," is defined as (i) identifiable information that vehicles collect, generate, record or store in electronic form that is retrieved from the vehicles by or on behalf of a Participating Member in connection with vehicle technologies and services;

---

[5] A copy of the Privacy Principles for Vehicle Technologies and Services can be found at http://www.autoalliance.org/index.cfm?objectid=865F3AC0-68FD-11E4-866D000C296BA163.

[6] Participating Members currently are: American Honda Motor Co., Inc.; Aston Martin Lagonda of North America, Inc.; BMW of North America, LLC; Chrysler Group LLC; Ferrari North America; Ford Motor Company; General Motors LLC; Hyundai Motor America; Kia Motors America, Maserati North America, Inc.; Mazda North American Operations; Mercedes-Benz USA, LLC; Mitsubishi Motors North America, Inc.; Nissan North America, Inc.; Porsche Cars North America; Subaru of America, Inc.; Toyota Motor Sales, USA; Volkswagen Group of America, Inc.; and Volvo Car Group.

[7] A copy of the 2013 GAO report can be found at http://www.gao.gov/assets/660/659509.pdf.

or (ii) personal subscription information provided by individuals subscribing to or registering for vehicle technologies and services.

(i) Transparency: Participating Members must provide vehicle owners and others who submit personal information in order to receive vehicle technologies and services (collectively, Users) with ready access to clear, meaningful notices about the Participating Member's collection, use and sharing of Covered Information. Such notices may be provided in a variety of ways, including in owners' manuals, on in-vehicle displays and via Web portals online. Participating Members must obtain the User's affirmative consent before using Covered Information in new and materially different ways. The notice needs to be clear with respect to the following areas:

- The types of Covered Information that will be collected;
- Why the Covered Information is collected;
- The types of entities with which the Covered Information may be shared;
- The deletion or de-identification of Covered Information, if applicable;
- Choices Users have as to Covered Information, if any;
- Access Users have to Covered Information, if any; and
- Where Users may direct questions about the collection, use and sharing of Covered Information.

The Principles also provide that the notice must also be prominent when (i) geolocation information (which reveals the precise geographic location of a vehicle); (ii) biometrics (such as touch-ID technology, which can reveal an individual's physical or biological characteristics); and (iii) driver behavior information (such as seat belt use, speed and braking habits) is collected.

(ii) Choice: Participating Members commit to offering Users certain choices regarding the collection, use and sharing of Covered Information. When geolocation, biometric or driver behavior information is collected, affirmative consent is required before such data can be used for marketing or provided to third parties for their own use. Affirmative consent is defined as a User's clear action in response to a clear, meaningful and prominent notice. The Principles do not further define what may constitute a "clear action."

(iii) Respect for Context: Participating Members commit to using and sharing Covered Information in ways that are consistent with the context in which the Covered Information was collected, taking account of the likely impact on Users. The Principles define "in context" as making reasonable and responsible use of the Covered Information in line with the explanation behind it (which may evolve over time). Reasonable and responsible practices include using or sharing Covered Information to diagnose or troubleshoot vehicle systems, provide requested or subscribed services, improve products and services, and prevent criminal activity.

(iv) Data Minimization, De-Identification and Retention: Participating Members commit to collecting Covered Information only as needed for legitimate business purposes and to retain Covered Information no longer than they determine necessary for legitimate business purposes.

(v) Data Security: Participating Members commit to implementing reasonable industry standard measures to protect Covered Information against loss and unauthorized access or use.

(vi) Integrity and Access: Participating Members commit to implementing reasonable measures to maintain the accuracy of Covered Information and commit to giving Users reasonable means to review and correct personal subscription information.

(vii) Accountability: Participating Members commit to taking reasonable steps to ensure that they and other entities that receive Covered Information adhere to the Principles. Such policies may take a number of forms, including training for employees and internal privacy review boards.

SKADDEN OBSERVATIONS

The Principles drew praise from a number of stakeholders. For example, the Auto Alliance release of the Principles included a quote from FTC Commissioner Maureen Ohlhausen praising the Principles as a means of allowing "consumers as well as industry members to benefit from [technology] advances without unintentionally slowing the pace of innovation." We expect to see an increasing number of industries turn to self-regulation as means of avoiding FTC regulation and providing comfort to customers as to the use of their information. It remains to be seen, however, whether such moves to self-regulation will be acceptable to data commissioners in other countries. The European Union, for example, has long taken a skeptical view toward self-regulation as a means of protecting individual privacy.

Return to Table of Contents

NIST RELEASES DRAFT GUIDE FOR SHARING CYBER-THREAT INFORMATION

Cybersecurity specialists in both the private and public sectors long have championed the importance of sharing information about cyber threats. The key benefit is readily obvious: Knowing about threats that others are facing will help an organization better prepare for and respond to cyber-attacks. On November 10, the National Institute of Standards and Technology (NIST) released a draft Guide to Cyber Threat Information Sharing (Guide) to help companies best facilitate such sharing.[8]

The goal of the Guide is to provide organizations with suggestions for establishing and maintaining information-sharing relationships throughout a cyber incident. To that end, the Guide highlights the benefits of information sharing while also noting some of the challenges to sharing, and presents the strengths and weaknesses of various information-sharing architectures.

The Guide includes some important suggestions on how organizations can facilitate information-sharing programs:

- Organizations should determine prior to an incident what information they have, what they can and cannot (*i.e.*, for confidentiality reasons) share with other parties, and under what circumstances information may be shared;
- When contemplating the sharing of information, organizations should consider:
  - The risks of disclosure;
  - Operational urgency and need for sharing;
  - Benefits gained by sharing;
  - Sensitivity of the information;
  - Trustworthiness of the recipients; and
  - Methods and ability to safeguard the information.
- Organizations should move from "informal, ad hoc, reactive" sharing approaches to formal, repeatable, adaptive, proactive and risk-informed ones.
- While there are benefits to sharing information through interpersonal meetings or contacts, organizations should consider using standard data formats and protocols to automatically exchange information. This allows for much faster sharing than interpersonal contacts and for diverse information from diverse sources to be correlated and analyzed. NIST recommends using technology standards that have been widely adopted.

[8] The draft Guide is available at http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-150http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-150.

- Combining internal and external information allows an organization to address a cyber incident throughout the "cyber-attack life cycle."
- Organizations should be prepared to commit personnel, hardware, software and the infrastructure needed to facilitate information sharing.
- Despite the importance of sharing information, organizations should implement security controls to protect sensitive information, as well as information obtained from third parties.

We anticipate that the final NIST Guide will be released in the coming months, but even in draft form, the Guide provides important guidelines for how organizations can maximize the benefits of information sharing.

Return to Table of Contents

SEC ADOPTS REGULATION SYSTEMS COMPLIANCE AND INTEGRITY

On November 19, the Securities and Exchange Commission adopted Regulation Systems Compliance and Integrity, 17 CFR 242.1000-1007 (Regulation SCI), which applies to self-regulatory organizations (including registered clearing agencies), alternative trading systems, plan processors and exempt clearing agencies. The entities covered by Regulation SCI must "establish, maintain and enforce written policies and procedures reasonably designed to ensure that their systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets, and operate in a manner that complies with the Exchange Act."

These plans must include:

- Reasonable current and future technology infrastructure capacity-planning estimates;
- Periodic capacity stress tests of such systems to determine their ability to process transactions in an accurate, timely and efficient manner;
- A program to review and keep current systems development and testing methodology for such systems;
- Regular reviews and testing, as applicable, of such systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters;
- Business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse, as well as reasonably designed, to achieve next business day resumption of trading and two-hour resumption of critical systems compliance and integrity (SCI) systems following a wide-scale disruption;
- Standards that result in such systems being designed, developed, tested, maintained, operated and surveilled in a manner that facilitates the successful collection, processing and dissemination of market data; and
- Monitoring of such systems to identify potential SCI events.

Regulation SCI-regulated entities must periodically review the effectiveness of its policies and take prompt action to remedy deficiencies in such policies and procedures. An organization's policies and procedures are deemed to be reasonably designed if they are consistent with current SCI industry standards, *i.e.*, the procedures follow practices widely available to information technology professionals in the financial sector and were issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization. The staff guidance lists examples of publications describing processes, guidelines, frameworks and standards available to an SCI entity seeking to comply with Regulation SCI. These include publications issued by NIST and the FFIEC.

The new rules provide a framework for regulated entities to take corrective action when security issues occur, provide notifications and reports to the SEC, inform members and participants about such issues, conduct business-continuity testing and conduct annual reviews of their automated systems.

The new rules will become effective 60 days after publication in the Federal Register, and entities will have nine months to comply (with certain extensions for alternative trading systems that are coming under Regulation SCI for the first time and for all organizations to comply with the industry- or sector-wide coordinated testing requirement).

Return to Table of Contents

FTC RESPONDS TO WYNDHAM'S APPEAL CHALLENGING ITS SECURITY REVIEW AUTHORITY

The FTC (or Commission) action against Wyndham Worldwide Corporation (Wyndham) has been the focus of many professionals in the privacy realm (as well as previous *Privacy & Cybersecurity Updates*), primarily because any decision, regardless of the outcome, is likely to significantly impact future FTC actions in the area of information security. In November 2014, another major development in this case took place — the FTC's filing of its response to Wyndham's interlocutory appeal of the District Court's refusal to dismiss the FTC complaint. The FTC's arguments give important insight into how it views the scope and basis for its authority in this arena, and may foreshadow the ultimate rationale of a Third Circuit decision on this issue.

BACKGROUND

The FTC/Wyndham action began in 2012 when the FTC issued a complaint against Wyndham related to three separate data breaches that occurred in 2008 and 2009. The FTC alleges that these incidents together exposed over 619,000 consumers to data theft and allowed hackers to rack up over $10 million in fraudulent charges. The FTC asserted its authority under Section 5 of the FTC Act and brought claims against Wyndham for allegedly engaging in both deceptive and unfair practices. Specifically, the FTC alleged that Wyndham harmed consumers by claiming to use commercially acceptable and industry-standard means for securing customer data while in reality failing to employ even basic security procedures.

Rather than settle with the FTC, as 50 other companies had done when faced with similar complaints, Wyndham moved to dismiss the claim. The company based its motion on three primary arguments:

- The unfairness standard under the FTC Act does not encompass unreasonable data security practices, and the Commission therefore lacked authority to regulate Wyndham's data breaches;
- The FTC had not given Wyndham constitutionally sufficient notice that its actions would be considered unfair; and
- The FTC's complaint did not sufficiently allege that the data breaches caused substantial consumer injury that the consumers could not have reasonably avoided.

The New Jersey District Court rejected all of these arguments and denied Wyndham's motion to dismiss the complaint. The court held that the FTC did have the general authority to regulate information security as an unfair trade practice, despite the absence of any specific cybersecurity laws or regulations granting this authority. Further, the court held that the Commission did not need to promulgate or announce specific rules or regulations regarding cybersecurity before bringing claims against companies.

In June, the district court certified the case for interlocutory appeal to the Court of Appeals for the Third Circuit, which in August agreed to hear the case. Wyndham's appeal focused on

the "unfair practices" provision of Section 5 and sought the Third Circuit's guidance on three crucial questions:

- Whether a company's unreasonable failure to protect the security of consumer data constitutes an unfair act or practice;
- Whether Wyndham had constitutionally sufficient notice that it needed to take reasonable steps to protect its consumer data; and
- Whether the FTC's complaint sufficiently alleged that the data breaches caused consumers substantial injury that they could not have reasonably avoided.

THE FTC'S RESPONSE

On November 5, the FTC filed its response to Wyndham's appeal. In the first section of its argument, the Commission asserted that a company's failure to implement reasonable data security practices constitutes an unfair practice, relying on a four-part analysis.

First, the FTC argued that Congress deliberately left broad the meaning of an "unfair act or practice in or affecting commerce" when it drafted and amended the FTC Act. The Commission argued that Congress recognized the pace at which businesses and individuals could devise new ways to act unfairly, and thus chose not to cabin the Commission with a specific definition that would be outdated as soon as it was codified.

Second, the FTC argued that Wyndham's "ordinary English" argument (suggesting that the definition of "unfair" requires "unscrupulous or unethical behavior") was untenable and contrary to both precedent and the FTC Act itself. The Commission pointed to several instances from cases and Congressional history highlighting the fact that intent or morality had been considered and rejected when defining "unfair" under the FTC Act.

Third, the FTC argued that the recent cybersecurity litigation considered and passed by Congress was meant to supplement, rather than displace or define, the FTC's current authority to regulate data-breach cases.

Finally, the FTC claimed that the Commission's previous determination that it has the authority to regulate cybersecurity issues deserved deference from the court under *Chevron USA, Inc. v. Natural Resources Defense Council, Inc.*, in which the Supreme Court held that courts should defer to agency interpretations of the statutes creating and guiding those agencies, unless the interpretations are unreasonable. Sitting in its capacity as an administrative tribunal in an action against LabMD,[9] the Commission rejected arguments similar to those Wyndham relied on, and it asserted that this determination of its own authority was not unreasonable and thus was due deference from the court.

In the second section of its argument, the FTC contended that Wyndham had fair and adequate notice of its responsibilities to reasonably protect its customers' data. First, the Commission argued that under ordinary common law and tort principles, Wyndham was on notice that it had a basic duty of care to its customers, and the violation of this same duty formed the basis for the FTC's complaint. Additionally, the Commission argued that it had given Wyndham (and all companies) specific notice through its previous complaints, previous consent judgments regarding data security and 2007 Guide for Businesses on Protecting Personal Information. The FTC asserted that these types of notice were constitutionally sufficient to satisfy due process.

Finally, the FTC argued that its complaint contained sufficient factual allegations to satisfy the pleading standard under the FTC Act. The Commission pointed to two primary categories of allegations from its complaint to support this point: (i) Customers faced unreimbursed charges

[9] We previously wrote about the LabMD action in the September 2014 edition of our *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_September_2014.pdf.

from the over $10 million in fraudulent charges that were attributable to Wyndham's actions, and (ii) even if customers were never held accountable for the fraudulent charges, they still spent time and money mitigating the harm caused by the breach of their data. The FTC contended that either of these types of harm on their own were sufficient to meet the pleading standard required to allege that Wyndham's actions caused consumers substantial injury that they could not have reasonably avoided.

LATEST UPDATES

While Wyndham's interlocutory appeal is being considered by the Third Circuit, the case has continued to proceed in the district court, and it now is in the discovery stage. However, the discovery process has been marked by several new disputes between the parties. As a result, on November 17, District Judge Esther Salas ordered the parties to participate in mediation before proceeding further with the case.

CONCLUSION

The Third Circuit's determination in this case will likely impact how both the industry and the FTC operate in the realm of data security. An FTC win could mean more aggressive enforcement in this area backed by an appellate court's endorsement that the Commission has broad authority to regulate. Conversely, a win for Wyndham could mean the Commission would focus more energy on the "deceptive practices" aspect of data breaches and could spur further congressional action in this field.

Return to Table of Contents

SKADDEN CONTACTS

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

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

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@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