Skadden

PRIVACY & CYBERSECURITY UPDATE

SEPTEMBER 2014

CONTENTS (click on the titles below to view articles)

Home Depot Data Breach — Lawsuits, Calls to Action and Lessons Learned 1

Skadden Participates in FBI Cyber-Intelligence Workshop 2

FTC Explores Impact of 'Big Data' on American Consumers in Public Workshop 3

Target Responds to Data Security Breach Class Action Suit by Credit Card Issuers . . . 4

Federal Court Allows California Customer Records Act Claims to Proceed Against Adobe. 6

Neiman Marcus Defeats Class Action Claim 8

FDIC Chairman Stresses Importance of Cybersecurity . . 9

U.S. Financial Services Industry Unites to Share Cyber Attack Information . . . 10

LabMD and Wyndham Continue to Challenge Broad FTC Security Review 11

The Potential Impact on Data Privacy of Recent Changes in the European Commission 14

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 15, or your regular Skadden contact.

HOME DEPOT DATA BREACH — LAWSUITS, CALLS TO ACTION AND LESSONS LEARNED

The recent data breach effecting Home Depot has attracted the now-all-too-common mix of media attention, negative publicity and class action lawsuits. This incident highlights the importance of establishing a cyber attack critical response plan and closely monitoring data security at the execution level.

As now confirmed by the company, Home Depot suffered a security breach affecting its payment systems that began in April 2014 and continued through September. During that period, according to the company, over 56 million credit cards were compromised, making this the largest known retail data breach to date. The alleged delay in detection and the volume of customers affected will undoubtedly fuel the class action and other claims against the company arising out of the attack. The company has said the cost of the breach will exceed $60 million, only some of which will be covered by insurance.

LITIGATION AND INVESTIGATION

While news of the breach broke out only recently, several class action lawsuits already have been filed against Home Depot in various jurisdictions. Indeed, the class action response was so rapid in this case that one putative class action suit was filed four days before Home Depot had publically confirmed the breach. The customer class action suits allege that Home Depot did not adequately protect consumer data and failed to alert consumers of the breach quickly enough. The named plaintiffs in one of the suits claim that they incurred fraudulent charges as a result of the breach, and reports of fraudulent activity resulting from the breach will undoubtedly lead to similar claims in other suits.

The Home Depot breach also is the subject of a class action suit filed by financial institutions. First Choice Federal Credit Union has filed a proposed class action lawsuit in the Northern District of Georgia on behalf of banks, credit unions and other financial institutions affected by the breach. The suit seeks damages resulting from having to cancel or reissue affected cards, close affected accounts or refund customers who experience unauthorized transactions as a result of the breach.

Finally, a group of attorneys general from states including New York, California, Illinois and Connecticut have launched an investigation of the breach. The investigation will focus on both the causes of the breach and the subsequent response by Home Depot, including how the retailer has dealt with affected consumers.

INCREASED LEGISLATIVE ATTENTION

As with the 2013 Target breach, the recent Home Depot incident has brought renewed legislative attention to the issue of information security. Senators Jay Rockefeller of West Virginia and Claire McCaskill of Missouri have cited the breach as further evidence that a federal data privacy bill is needed. Senators Richard Blumenthal of Connecticut and Edward Markey of Massachusetts have drafted a letter to FTC Chairwoman Edith Ramirez urging an investigation into the breach and questioning the data protection measures Home Depot had in place.

The White House, citing the Home Depot breach among other events, in September characterized cybersecurity as one of the greatest national security dangers the United States

faces. The administration has taken a number of steps to increase federal cybercrime prosecution, and to identify and mitigate cyber threats, but also has suggested that additional federal legislation is required.

Whether these increased calls to action will be enough to break through philosophical and political differences in enacting legislation remains to be seen. In the meantime, governmental bodies such as the Federal Trade Commission, the Department of Health and Human Services, and the Office of the Comptroller of the Currency may try to step up their enforcement efforts using the legal tools already available to them.

LESSONS LEARNED

Have a Rapid Response Plan in Place

The Home Depot breach, which follows on the heels of recent breaches at Target, Neiman Marcus, P.F. Changs and others, serves as an important reminder that companies need to evaluate their own data protection policies and implement rapid response plans to handle cyber attacks. With new, massive data breaches being announced with increasing frequency, boards and senior management at companies can no longer claim to be unaware of the threats and should be sure to take steps to ensure that adequate protections are in place.

In addition, in what is becoming a familiar pattern, news of the breach was first reported by security blogger Brian Krebbs. This fact demonstrates the changing landscape and narrowing timeframe that companies have in which to respond to attacks. Companies are increasingly likely to learn of a breach when news of it is posted online or through other means, rather than through their own investigations. When a breach is publicized by a third party, the company itself may lose control of the narrative, which may undermine the company's credibility with the public. It therefore is critical that companies have in place rapid response plans to address these events when they happen.

Everyone Is Vulnerable

The facts and circumstances leading to the Home Depot breach have not yet been disclosed, but recent events have shown that all companies are vulnerable to cyber attack. Even after large, well-publicized breaches such as the Target incident in the winter of 2013-2014, prompting companies and vendors to examine their systems and patch vulnerabilities, new breaches are being announced nearly every week. Cyber attackers continue to develop new methods and discover new vulnerabilities to exploit, and companies must remain vigilant and constantly evaluate and update their security protections.

Return to Table of Contents

SKADDEN PARTICIPATES IN FBI CYBER-INTELLIGENCE WORKSHOP

On September 16, 2014, Stuart Levi, the head of Skadden's Privacy and Cybersecurity Group, spoke at a cyber-intelligence workshop coordinated by the FBI's cyber division. Stuart spoke on a panel that highlighted the importance of cooperation between the FBI and the private sector in thwarting cyber attacks. Stuart's focus was on the deliberations that companies go through before contacting the FBI after a cyber attack. Throughout the day-long program, FBI agents and security professionals highlighted the growing cyber threat, both domestically and internationally, and the critical role that law enforcement can play when a company is attacked. The program, and outreach efforts by the FBI to the private sector, highlight that the FBI very much views itself in a partnership role with companies, organizations and other law enforcement bodies in the area of cybercrime. Companies that have been attacked always should give serious consideration to the role of law enforcement, and they may even consider reaching out to law enforcement before an attack occurs to establish an ongoing relationship.

Return to Table of Contents

FTC EXPLORES IMPACT OF 'BIG DATA' ON AMERICAN CONSUMERS IN PUBLIC WORKSHOP

On September 15, 2014, the Federal Trade Commission hosted a public workshop entitled "Big Data: A Tool for Inclusion or Exclusion?" to examine how companies use "big data" to predict consumer behavior, possibly to the detriment of low-income and underserved populations. The FTC's decision to host this workshop reflects its continuing interest in this subject and suggests that the Commission intends to develop recommended practices — or possibly regulations — in this area.

The term "big data" refers to the vast and complex pools of information being collected and stored by various public and private bodies. Its importance has grown in recent years due to the widespread use of social media, smartphones and the Internet, which collect data from their users for various purposes. Companies can use big data to predict consumer behavior patterns to more effectively target advertisements or promotions. For instance, companies may offer specific discounts to consumers based on spending patterns or gear advertisements for financial products towards individuals at certain income levels. Similarly, governments can use big data to shape policy and establish priorities, such as using traffic data to identify areas where increased road maintenance is needed.

Big data has been a recent topic of discussion among government officials. On May 1, 2014, the White House released two reports, one exploring the benefits and risks of big data, and the other examining how big data can be used to solve various technology issues.[1] Just a few days before the public workshop, FTC Commissioner Julie Brill gave an address at the Mentor Group Vienna Forum on big data and related developments in privacy entitled "Privacy in the Age of Omniscience: Approaches in the United States and Europe."

While companies may view big data as a way to more efficiently tailor their products towards consumers who will more likely purchase them, many people are concerned that companies are using big data to unfairly impede low-income and underserved populations from accessing higher quality products and services. For example, financial institutions may offer sub-prime credit cards to low-income consumers and reserve more attractive offers for consumers with higher incomes. FTC Chairwoman Edith Ramirez noted in her opening remarks at the workshop that big data "has the capacity to save lives, improve education, enhance government services, increase marketplace efficiency and boost economic productivity," but that it also can "reinforce disadvantages faced by low-income and underserved communities. As businesses segment consumers to determine what products are marketed to them, the prices they are charged and the level of customer service they receive, the worry is that existing disparities will be exacerbated."[2]

The workshop examined the potential impact of big data on disadvantaged populations, as well as possible solutions to address and reduce the potential risks. The key points to emerge from the workshop include:

- **Using existing legal frameworks to stop discriminatory uses of big data**. Currently, there are no federal laws preventing and punishing use of big data in a discriminatory manner. However, the Civil Rights Act (CRA) and the Equal Credit Opportunity Act (ECOA) each could be applied to such situations. For example, the CRA's "disparate impact" analysis could be used to determine whether use of big data to screen applicants for jobs is a business necessity. In addition, using big data to withhold credit from creditworthy applicants based on race, color, religion, national origin, sex, marital status or age could result in civil liability under the ECOA.

---

[1] These reports are discussed in detail in our May 2014 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_May_2014.pdf.

[2] FTC Chairwoman Edith Ramirez, "Big Data: A Tool for Inclusion or Exclusion?", Washington, D.C., Sept. 15, 2014, available at http://www.ftc.gov/system/files/documents/public_statements/582421/big_data_workshop_opening_remarks_ftc_chairwoman_edith_ramirez_9-15-14.pdf.

- **Self-regulation in the use of big data.** Several panelists discussed the role of self-regulation, highlighting that companies want to appear ethical and use big data responsibly so that they remain accountable to the public. For example, members of the Direct Marketing Association (DMA), a trade organization that promotes responsible, data-driven marketing, must comply with strict guidelines that govern data use. The DMA also publishes a list of "bad actors" that fail to comply with the DMA's policies. Self-regulation can be used to fill the gaps in current laws that do not directly address the use of big data in discriminatory ways.
- **Legislation addressing big data use issues not necessarily on the horizon**. While panelists discussed various legal and self-regulatory paths towards ensuring the proper use of big data, there was no indication that new legislation or federal regulation directly addressing big data issues is forthcoming.

PRACTICE POINT: ONGOING REVIEW

The increased focus on big data during 2014 suggests that policymakers are likely to take action to curb the abuse of big data in the relatively near future. Whether this action will be in the form of new regulation, increased enforcement of existing law, encouragement of self-regulation or some combination thereof remains to be seen, but companies that seek to use this data in their businesses should be mindful of any disparate impacts that may result. Companies interested in this issue should note that the FTC is accepting written comments on issues related to this workshop until October 15, 2014.

Return to Table of Contents

TARGET RESPONDS TO DATA SECURITY BREACH CLASS ACTION SUIT BY CREDIT CARD ISSUERS

As has been widely reported, the cyber attack on Target in late 2013 resulted in multiple lawsuits with many individuals and entities allegedly harmed by the massive data breach seeking to shift the liability for these harms onto others. One such case, I*n re: Target Customer Data Security Breach Litigation (All Financial Institutions)*,[3] was brought in Minnesota by federal court "issuing banks" — *i.e.*, banks that issued the credit cards from which the data was stolen — as a result of having to subsequently cancel and reissue such credit cards at great cost.

As we noted in our January 2014 *Privacy & Cybersecurity Update*,[4] issuing banks typically argue that merchants should bear these costs, since it was a failure of the merchants' security that resulted in the breach. Merchants take the opposite view and argue that it is the issuing banks who should bear the cost of these breaches, as the banks have chosen not to issue cards with appropriate levels of security protection, which could mitigate or even prevent the harms caused by these types of breaches.

On September 2, 2014, Target filed a Memorandum of Law in Support of Motion to Dismiss the Consolidated Class Action Complaint, arguing that each of the issuer banks' theories of liability falls short of stating a claim for relief.

CHALLENGES FACED BY ISSUERS

The indirect nature of the relationship between Target and the issuing banks lies at the heart of the challenges that the plaintiff issuing banks face in prevailing on their claims. Here, the issuing banks have no contractual or other direct legal relationship with Target. Instead,

---

[3] MDC No. 14-2522.
[4] Available at http://www.skadden.com/newsletters/Privacy_and_Cybersecurity_Update_January_2014.pdf.

issuing banks have contracts with the consumers who use the credits cards issued by the issuing bank. The issuing banks also have contractual relationships with the various credit card brands, such as Visa and Master Card. When a consumer pays for a purchase at a merchant such as Target, the merchant communicates with an "acquiring bank" — a different bank than the issuing bank that has a contractual relationship with the merchant. The acquiring bank communicates with the applicable card brand to obtain authorization and funding under the acquiring bank's contract with the card brand. Finally, the card brand turns to the issuing bank to receive authorization and funding pursuant to the card brand's contract with the relevant issuing bank.

Due to this lack of privity of contract with Target, the issuer banks base their claims on various theories of negligence — *i.e.*, that Target's actions or omissions resulted in harm to the issuer banks, such that Target should be held liable for such harm.

NO "SPECIAL RELATIONSHIP" OR PRIVITY

The core of Target's response to the issuers' negligence claims is that, because of the indirect nature of the relationship between Target and the issuing banks, Target owed no duty of care to the issuing bank .

Target's Memorandum emphasizes that, in order for a court to find Target liable under a negligence or negligent misrepresentation theory, the court would have to recognize a new "special relationship" between issuing banks and merchants that would impose upon merchants a duty to protect against third-party criminal harm. This seems unlikely to occur, Target's argument continues, in light of the fact that: (i) the Minnesota Legislature already addressed this issue in existing legislation and determined not to impose such a duty on merchants; (ii) the issuing banks already have contractual remedies available to them pursuant to their existing agreements with card brands; and (iii) courts in other jurisdictions have refused to impose duties on merchants in situations similar to the one at bar.

NO VIOLATION OF MINNESOTA STATUTE

In addition to their theories of negligence, the issuers claimed that Target violated Minnesota's Plastic Card Security Act and that they suffered injury as a result of such violation. Target responded that PCSA only applies where a merchant has retained certain card data after a payment transaction is authorized and that the issuing banks had not established that Target retained any of that information or that any such stored data was affected by the data breach. As the issuers acknowledged, the malware installed on Target's systems stole payment data in real time.

ECONOMIC LOSS DOCTRINE NOT ASSERTED

Target elected not to assert a defense based on the economic loss doctrine, which provides generally that one cannot recover in tort for a purely economic loss that is not a consequence of some bodily harm or damage to property.[5] In all likelihood, Target's decision not to assert this doctrine as a defense to the issuers' claims was driven by local law considerations. Minnesota has abrogated and severely limited the common law doctrine by statute, so purely economic losses are, in fact, recoverable in some circumstances.[6] Minnesota is not alone in this position. In 2013, the Fifth Circuit held in *Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*[7] that New Jersey's limited formulation of the economic loss doctrine did not preclude claims of foreseeable economic loss by an issuer bank against a processor of credit card transactions arising from a cybersecurity attack on the processor. Nevertheless, application of the economic loss doctrine as a defense to claims of pure economic loss arising from cybersecurity attacks may remain viable in those jurisdictions that are more hospitable to the doctrine.

---

[5] *See, e.g.*, Restatement (Third) of Torts: Liab. for Econ. Harm § 1(a) TD No. 1 (2012) ("An actor has no general duty to avoid the unintentional infliction of economic loss on another").
[6] *See Ptacek v. Earthsoils, Inc.*, 844 N.W.2d 535, 538-39 (Ct. App. 2014).
[7] 29 F.3d 421 (5th Cir. 2013).

CONCLUSION

Target's response to the issuing banks' suit demonstrates some of the ambiguities surrounding liability for these types of retail data breaches, whether under common law or under statute. As the number of high-profile breaches and related lawsuits continues to grow, a variety of courts are likely to have an opportunity to rule on these issues. Companies that use, collect, transmit, store or process personal data should continue to monitor this case and others like it, as such cases seek to challenge and reshape existing law to address new issues that arise out of big data and other new technologies.

Return to Table of Contents

FEDERAL COURT ALLOWS CALIFORNIA CUSTOMER RECORDS ACT CLAIMS TO PROCEED AGAINST ADOBE

In *In re: Adobe Systems, Inc. Privacy Litigation*[8], Judge Lucy Koh of the U.S. District Court for the Northern District of California granted in part and denied in part claims alleged against Adobe under the California Customer Records Act (the CRA) and the California Unfair Competition Law (UCL), as well as a claim for declaratory relief, arising out of a 2013 data breach of Adobe customers' personal information stored on Adobe's servers. The *Adobe* ruling reaffirms Ninth Circuit precedent regarding Article III standing in light of recent United States Supreme Court rulings and underscores the importance of investment in security measures that comply with industry standards.

BACKGROUND

Adobe is a software company that sells and licenses printing, publishing, multimedia and graphics software. Adobe collects a variety of types of customer information, such as names, email and mailing addresses, credit card numbers and expiration dates, passwords and telephone numbers. In addition, some Adobe subscription customers also store their files and work product in Adobe's "cloud."

In July 2013, hackers gained entry into Adobe's servers without detection and spent several weeks there undetected, removing customer data and Adobe source code. In September, independent security researchers discovered the data breach; however, Adobe did not announce the breach until October 3, 2013.

Plaintiffs alleged that Adobe violated the CRA and the UCL by failing to: (a) maintain "reasonable security practices" to protect customer data (Cal. Civ. Code § 1798.81.5); and (b) promptly notify customers following the 2013 data breach (*id.* § 1798.82). Plaintiffs also sought a declaratory judgment that Adobe is currently in breach of existing contractual obligations to provide reasonable security measures.

THE COURT'S RULING

Article III Standing: Krottner v. Starbucks Corp. *remains the law of the Ninth Circuit*

The plaintiffs alleged that they suffered three types of cognizable injuries-in-fact to support standing: (1) increased risk of future harm; (2) cost to mitigate the risk of future harm; and/or (3) the loss of value of their Adobe products.

Citing multiple district court data breach opinions, Adobe argued that increased risk of future harm is insufficient to establish Article III standing after *Clapper v. Amnesty International USA*,

[8] No. 13-CV-05226-LHK (N.D. Cal. Sept. 4, 2014).

133 S. Ct. 1138 (2013), in which the U.S. Supreme Court held that the plaintiffs — human rights lawyers, labor, legal and media organizations concerned that their communications with foreign nationals might be intercepted by the government under Section 702 of the Foreign Intelligence Surveillance Act of 1978 — lacked Article III standing because the harm they envisioned was not "certainly impending."

Judge Koh rejected the argument, reaffirming *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) as the law of the Ninth Circuit. Judge Koh held that *Krottner*'s "credible threat of real and immediate harm" standard was not inconsistent with *Clapper*. In addition, Judge Koh held that both standards (if they are different) would be satisfied because the hackers specifically targeted Adobe's network in order to steal personal information, actually stole the information and successfully decrypted the information, some of which already had surfaced on the Internet. Thus, the threat of future harm was "certainly impending," and far greater than the "highly speculative fear" of the *Clapper* plaintiffs that a government agency *might* intercept some of their communications. Judge Koh distinguished other district court cases on the ground that in most of them it was unclear whether the thief was targeting the data or just the device on which it was stored (*e.g.*, the laptop).

Judge Koh also held that because the risk of future harm was imminent and certain, the costs of mitigation incurred by two plaintiffs for data monitoring services constituted an additional injury in fact (*i.e.*, the plaintiffs had not attempted to manufacture standing by incurring the costs to injure themselves). However, the court dismissed the plaintiffs' Section 1798.82 claim for failure to reasonably notify customers of the 2013 data breach because they did not allege that they suffered any *incremental harm* as a result of the delay in notification.

Declaratory Relief Proper to Address Allegedly Inadequate Security Practices

Rejecting Adobe's argument that the plaintiffs sought an advisory opinion to gain an advantage in future litigation, the court refused to dismiss the plaintiffs declaratory relief claim that Adobe's *current* security measures breached current contractual obligations. The court also rejected out of hand Adobe's argument based on a disclaimer in its End User License Agreement (EULA) that "no security controls are 100 percent effective and Adobe cannot ensure or warrant the security of your information," holding that such disclaimer did not relieve Adobe of its responsibility under the EULA to provide "reasonable" security.

Deficient Security Practices Stated California UCL Claim

California's UCL broadly covers any unlawful, unfair or fraudulent conduct. The court held that the plaintiffs stated a claim under the UCL based on their alleged injury-in-fact (see standing discussion above) and the alleged violation by Adobe of California's CRA (which satisfied both the unlawful and unfair prongs of the UCL). Adobe argued that the plaintiffs lacked statutory standing under the UCL because they did not allege that they personally lost money or property as a result of unfair competition. The court held that four plaintiffs adequately alleged that they spent more on Adobe products than they would have had Adobe disclosed its deficient security, but dismissed with leave to amend as to those plaintiffs who did not.

Plaintiffs Stated California UCL Restitution Claims

Judge Koh held that although the plaintiffs had not purchased Adobe's more expensive, license-based ColdFusion product (they purchased the less expensive Creative Cloud product), the products were substantially similar for standing purposes because both were allegedly "heavily security-dependent." Thus, the relevant issue was "whether purchasers of [both] products valued security, and thus whether they overpaid for their Adobe products in light of Adobe's alleged misrepresentations and omissions regarding security." Accordingly, the Plaintiffs had standing to represent a class of purchasers of both productions.

Adobe argued that the plaintiffs failed to allege a "fraudulent" statement under the UCL because its inadequate security had been widely publicized and thus it had no duty to disclose such information (*i.e.*, such information was no longer "exclusively" known to Adobe, as required by California law). The court held that Adobe's poor reputation for security in general did not mean the specific security shortcomings at issue were widely known, finding cited reports in *CNN Money*, the *New York Times, the Wall Street Journal* and *Reuters* to be "highly generic." The court further held that the exact nature of what was in the public domain was a question of fact not properly resolved on a motion to dismiss.

Finally, the court held that the plaintiffs satisfied the "unfair" prong of the UCL by alleging that Adobe gained an unfair competitive advantage by failing to make adequate expenditures on security measures that complied with industry standards when its competitors were required to do so.

PRACTICE POINTS

For companies that maintain and utilize sensitive consumer information, this lawsuit highlights the importance of continually updating and investing in security practices. As the *Adobe* opinion made clear, disclaimers that the company cannot guarantee the safety of the consumer are unlikely to provide protection from liability in the event of a data breach, if the company's security practices are considered inadequate by industry standards.

Return to Table of Contents

NEIMAN MARCUS DEFEATS CLASS ACTION CLAIM

In another blow to class actions brought against companies that suffer data breaches, an Illinois district court judge dismissed a putative class action claim against Neiman Marcus, finding that the plaintiffs lacked standing.

BACKGROUND

In *Remijas v. The Neiman Marcus Group, LLC*, Case No. 1:14-cv-01735 (N. D. Ill.), the plaintiffs sued Neiman Marcus for negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy and violation of several state data breach acts arising from a 2013 cyber attack in which 350,000 customers' payment card data and personally identifiable information was stolen. The plaintiffs alleged that Neiman Marcus failed to adequately protect against such a security breach, and failed to provide timely notice of the breach once it happened.

The plaintiffs claimed both future and present injuries. First, they claimed they were injured through an increased risk of future fraudulent credit card charges and identity theft. Second, they asserted present injuries of the loss of time and money associated with resolving fraudulent charges and protecting against the risk of identity theft, financial loss from having purchased products that they wouldn't have purchased had they known of Neiman Marcus' misconduct, and the loss of control over their personal information. Neiman Marcus countered that none of these claimed injuries conferred Article III standing and moved to dismiss.

In granting Neiman Marcus' motion, Judge Zagler acknowledged that that allegations of future potential harm can establish Article III standing, but only if the future harm is "certainly impending." Analyzing the facts before it, the court noted that since "the overwhelming majority" of plaintiffs only allege that their data *may* have been stolen, it is difficult to conclude that harm is certainly impending. However, the court also noted that Neiman Marcus conceded that approximately 2.5 percent of the 350,000 customers whose information was breached did, in fact, suffer fraudulent charges.

Based on these facts, the court first concluded that plaintiff's "fear of identity theft" claim could be dismissed since the fraudulent charges did not render identity theft a "certainly impending" injury. The court next concluded that even the 2.5 percent who confronted fraudulent charges were not able to establish "concrete" injury, since all of those claims were reimbursed. The lack of concrete injury meant that Article III standing was not satisfied.

With respect to the plaintiffs' argument that they also are suffering current injury because of "time and money spent" to protect against fraudulent charges and identity theft, Judge Zagler acknowledged that money spent to prevent future harm could confer Article III standing. However, this is only in cases where the future harm is a cognizable Article III injury. Since that does not exist in this case, plaintiffs are not currently being harmed.

Judge Zagler also dismissed as "creative but unpersuasive" plaintiff's argument that Neiman Marcus overcharged for products since part of the overhead for each product should have been spent on cybersecurity, but apparently was not (given the breach). As the court noted, a "vital limiting principle" to plaintiff's theory "is that the value-reducing deficiency is always intrinsic to the product at issue." Here, the deficiency — poor security — was extrinsic to the product being purchased.

The Neiman Marcus case demonstrates that while plaintiffs are often quick to bring class actions against retailers and other entities who have suffered a data breach, establishing Article III standing still remains a significant roadblock in many cases.

Return to Table of Contents

FDIC CHAIRMAN STRESSES IMPORTANCE OF CYBERSECURITY

In remarks to the American Banker Regulatory Symposium on September 22 , 2014, concerning issues of critical importance to the U.S. banking industry, FDIC Chairman Martin J. Gruenberg focused in part on cybersecurity.

Chairman Gruenberg stressed that cybersecurity is "the most urgent category of technological challenges facing banks" and a key component of managing operational risks for both large and small banks. He reminded banks that the supervisory processes for conducting IT examinations is well-established and that, in partnership with the Federal Financial Institutions Examination Council (FFIEC), the FDIC "has developed a framework for conducting IT examinations that covers a broad spectrum of technology, operational and information security risks." This framework consists of "published standards, examination procedures, routine on-site inspections and enforcement capability," as well as a series of Information Technology Examination Handbooks that communicate regulatory expectations for IT and information security.

Most importantly, Chairman Gruenberg pointed out that cybersecurity is no longer just an IT issue, but rather "needs to be engaged at the very highest levels of corporate management." This concept has been echoed by numerous regulators and is a focal point of the NIST Framework for Improving Critical Infrastructure Cybersecurity.

Chairman Gruenberg then proceeded to highlight some of the key developments in the financial services regulatory environment as it relates to cybersecurity:

- In June 2013, the FFIEC formed a new Cybersecurity and Critical Infrastructure Working Group to serve as a liaison with the intelligence community, law enforcement and the Department of Homeland Security on issues related to cybersecurity and the protection of critical infrastructure. The goal of the Working Group is to help the banking agencies collaborate in developing examination policy, training and information sharing, and coordinating responses to cybersecurity incidents. The Working Group also is undertaking an assessment of the banking sector's overall readiness to address a significant cyber threat.

- The FDIC has initiated a number of programs this year to assist community banks in their awareness of cyber threats and to provide practical tools to help mitigate these risks.
- The FDIC has begun requiring third-party technology service providers to update their client financial institutions on any operational concerns the FDIC identifies when the service providers are examined.

The chairman also encouraged banks to practice responding to cyber threats as part of their regular disaster planning and business continuity exercises.

Return to Table of Contents

U.S. FINANCIAL SERVICES INDUSTRY UNITES TO SHARE CYBER ATTACK INFORMATION

In an effort to reduce the threat of cyber attacks to the industry, a group of U.S. financial institutions have created a software platform to share cyber threat information. The companies hope that by increasing the amount of information shared and improving the dissemination of such information they will be able to increase their collective ability to thwart future attacks.

Security experts have long favored a policy of increased information sharing among cyber attack targets to enable them to better understand existing attack methods, identify new attack methods, and identify security vulnerabilities in their own systems. Some companies historically have been reluctant to share this type of information, citing competition issues, the fear of disclosures being used in litigation and concerns over maintaining confidentiality. The U.S. government has tried to encourage information sharing through initiatives such as the Department of Homeland Security's Enhanced Cybersecurity Services, and has been proactive in notifying companies of specific attacks against them as well as attack trends. The government's efforts are limited, however, by its ability to identify attacks independently and by the scope of information voluntarily shared by U.S. companies.

Under this new initiative, the Financial Services Information Sharing and Analysis Center (FS-ISAC) will partner with the Depository Trust and Clearing Corporation to create a joint venture, known as Soltra, to launch a software platform. This platform, which will be known as Soltra Edge, is intended to collect, distill and speed the transfer of threat information from a number of sources. Although it does not solve all of the limitations of the existing information sharing regime, Soltra Edge is intended to both encourage and facilitate communication within the industry.

Some have expressed concern that this initiative — which initially will be a pilot program limited to only 45 organizations — will create a class of cybersecurity haves and have-nots, with smaller financial services firms not having access to the same quality and volume of information as the major firms. Should the program prove successful, however, other firms may seek to join the effort, and others in the financial services or other industries may choose to establish their own programs.

Soltra represents only the latest effort by the private sector to take steps to protect itself against cybersecurity threats. As attacks continue despite government efforts to reduce the threat, additional efforts such as these are likely to develop.

Return to Table of Contents

LABMD AND WYNDHAM CONTINUE TO CHALLENGE BROAD FTC SECURITY REVIEW

Two companies that have come under FTC scrutiny for their handling of consumer information continue to challenge the scope of the FTC's authority to impose penalties for data-security practices. Hotel chain owner Wyndham Worldwide and cancer-testing laboratory LabMD are each targets of FTC enforcement actions, and each is continuing to press its legal argument that the FTC does not have the authority to enforce certain data security standards against them. Both cases have undergone various twists and turns, but the outcomes could significantly impact the FTC's efforts to police data security practices.

BACKGROUND

As reported and discussed in a number of prior *Privacy & Cybersecurity Updates*, the FTC has asserted broad authority under Section 5 of the FTC Act to sanction companies that engage in unfair or deceptive acts or practices with respect to data security.[9] The Commission has had considerable success in this area, with more than 50 companies entering into settlement agreements to date.

Broadly speaking, the Commission has claimed general authority to take action in two separate types of data security claims, though it often asserts both in individual cases:

- **Unfair acts or practices:** Where (a) a company's data security practices cause or are likely to cause substantial injury to consumers, (b) the injury cannot be reasonably avoided by the consumers, and (c) the injury is not outweighed by countervailing benefits to consumers or competition.
- **Deceptive acts or practices:** Where (a) a company has made a representation or omission, or has engaged in a practice, that is likely to mislead consumers, (b) a consumer's interpretation of the representation, omission or practice is reasonable under the circumstances, and (c) the misleading representation, omission or practice is material.

Using this claimed authority, the FTC has settled claims against a wide range of companies related to a variety of practices. The underlying facts have included failure to follow proper security procedures, inaccurate statements in privacy policies and security claims in promotional materials that do not match the level of information security actually in place.

Rather than settle, however, Wyndham and LabMD have gone to court to challenge the FTC's authority to take action against them for information security practices.

WYNDHAM HOTELS

The FTC's action against Wyndham arises out of data breaches experienced at a number of hotels dating back to 2008, through which attackers gained unauthorized access to credit card numbers and other personal information concerning Wyndham guests. The Commission alleged that Wyndham had engaged in deceptive and unfair practices by (a) claiming to use industry standard measures to protect information when, according to the FTC, Wyndham failed actually to do so, and (b) implementing a variety of flawed security procedures and not remedying issues even after they came to light.

Wyndham Challenge to FTC Authority

Wyndham moved to dismiss the FTC claim, arguing that the Commission does not have the authority to regulate data security practices under the FTC Act's unfairness standard. Among other arguments, Wyndham asserted that:

---

[9] *See, e.g.* our February 2014 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_February_2014.pdf.

- Congress had passed narrowly tailored privacy legislation giving the Commission specific information-security authority in specific areas and had recently proposed a number of bills giving the FTC broader cybersecurity authority, so the Commission cannot claim that Congress intended to give it broad authority; and
- The FTC had not issued sufficient regulations and guidance to companies to enable them to determine what the FTC required with respect to information security.

FTC Victory

In a clear victory for the FTC, the court rejected Wyndham's claims in April, ruling that:

- The FTC has general authority to regulate information security as an unfair trade practice under the FTC Act even though there are no specific cybersecurity laws or regulations granting the Commission this general authority; and
- The FTC does not need to promulgate rules or regulations regarding cybersecurity standards before it can bring a claim.[10]

Third Circuit Appeal

In June, the *Wyndham* court certified the case for interlocutory appeal to the Court of Appeals for the Third Circuit, and in August the court agreed to hear the case to resolve two critical issues:

- Whether the FTC can bring an unfairness claim involving data security under the FTC Act; and
- If so, whether it must formally promulgate regulations before bringing its unfairness claim under the Act.

The court has not yet announced a date for oral arguments.

LABMD

Though garnering less publicity than the *Wyndham* case, LabMD's ongoing battle with the FTC could end with important decisions regarding the Commission's authority to regulate information security in areas arguably already within the jurisdiction of other agencies.

The case began in 2010, when the FTC began an investigation of cancer-testing company LabMD after medical and personal information for nearly 9,000 patients had been made available over a peer-to-peer file sharing service. The Commission was tipped off to this disclosure by Tiversa, a file-sharing intelligence firm that allegedly discovered the information online in 2008.

In January 2014, LabMD announced it was winding down its operations — citing the burden of the FTC case — but has continued to battle the Commission's claims against it.

LabMD Challenges FTC's Authority With Respect to Health Information

LabMD filed multiple motions to dismiss the case, some of which raise novel arguments against FTC authority over LabMD. The company argued that even if the FTC has general authority to regulate data privacy under Section 5 — which LabMD contests on largely the same grounds as Wyndham — the Commission does not have authority in the health-information area because Congress delegated sole enforcement authority in that area to the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), each of which authorizes the HHS to establish and enforce information security standards.

---

[10] We described this decision in greater detail in the April 2014 edition of our *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_April_2014.pdf.

If LabMD is successful in this argument, the FTC's authority to enforce broad security standards under the unfairness doctrine may be limited to areas where authority over information security has not already been delegated to another agency. Areas outside the FTC's jurisdiction might include, for example, health information and information held by financial services companies.

The various district courts and appellate courts have so far refused to dismiss the FTC's case against LabMD but have done so largely over procedural and standing issues — so far, they have not fully addressed LabMD's claims.[11]

Challenges to FTC's Evidence

In the late spring of 2014, however, just as an administrative trial was beginning, the case took an unusual turn: The House Committee on Oversight and Government Reform began investigating Tiversa's involvement in the case and called current and former Tiversa employees to testify. In a June 2014 letter to the FTC's acting inspector general, Committee Chairman Darrell Issa made a number of startling allegations, citing testimony before the Committee, including that Tiversa:

- had alerted the FTC of the security breach only after LabMD refused to hire Tiversa to remediate the breach;
- had created a special group in conjunction with the FTC specifically to provide information regarding data breaches in response to FTC investigative demands; and
- may have manipulated information to advance FTC investigations, and may not have been truthful in testimony it provided to federal government entities.

As a result, Issa claimed that the Committee had "substantial concerns" about the reliability of the information Tiversa provided and the relationship between Tiversa and the Commission. There also was some suggestion that other companies had received FTC inquiries shortly after refusing to hire Tiversa for security remediation services.

In response to these revelations, the administrative trial was adjourned. LabMD sought sanctions against the FTC in relation to its handling of the evidence Tiversa provided, but the administrative law court declined to take action because it found too much uncertainty regarding the assertions of Tiversa misconduct.

Should the FTC's case survive these allegations of misconduct, the administrative law judge will be left to decide key issues involving the FTC's authority over information security practices.

IMPACT OF DECISIONS

Whatever the outcome, the Wyndham and LabMD cases against the FTC could significantly impact future FTC actions in the area of information security.

- A loss for the FTC would likely spell a greater Commission emphasis on allegedly deceptive information security practices, perhaps with an enhanced focus on generalities such as assurances that a company uses "industry standard" security practices. It also would likely provoke increased efforts by the Commission to influence and encourage comprehensive information security legislation from Congress.
- An FTC win could lead to more aggressive enforcement action in this area and perhaps a reduced sense of urgency for additional federal legislation on information security practices generally.

---

[11]The LabMD case is described in further detail in our December 2013 *Privacy & Cybersecurity Update* (available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Alert_December_2013.pdf) and our May 2014 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_May_2014.pdf.

Return to Table of Contents

THE POTENTIAL IMPACT ON DATA PRIVACY OF RECENT CHANGES IN THE EUROPEAN COMMISSION

The European Commission, one of the three main EU legislative bodies, currently is in the midst of a complete overhaul. Every five years, the 28 European Commission members (one for each member state) change through a somewhat elaborate process. Jean-Claude Juncker, the incoming president of the Commission, was selected by the Council of the EU. Juncker now must select and assign positions to the other 27 members. The Council and the European Parliament must approve Juncker's selections and plan. In this cycle, Juncker has opted to restructure the European Commission by allocating the 27 other commissioners among two "high vice presidents," five vice presidents and 20 commissioners. Seven vice presidents will head up project teams to oversee and coordinate the commissioners.

From a data privacy perspective, a key selection is Andrus Ansip, the former Estonian prime minister, who will be vice president for the "Single Digital Market" project. In his mission letter from Juncker, Ansip is tasked with steering and coordinating the work of several commissioners, including the commissioners for Digital Economy and Society; Internal Market, Industry, Entrepreneurship and SMEs; Employment, Social Affairs, Skills and Labour Mobility; Justice, Consumers and Gender Equality; Economic and Financial Affairs, Taxation and Customs; Regional Policy; and Agriculture and Rural Development. After stressing the importance of enhancing the EU's role in the global digital economy, Juncker notes that companies will need to be subject to the same data protection and consumer rules, regardless of where their servers are based. Ansip also is assigned to build "the framework conditions" that will allow EU citizens to "enjoy the same freedoms and protections online as they have offline, including by working to fight cybercrime."

Most importantly, Juncker tasks Ansip with overseeing, *during the first six months,* the conclusion of negotiations on the reform of Europe's data protection rules as well as the review of the Safe Harbor arrangement with the U.S. Whether this formal guidance will speed up the enactment of a new EU data protection directive or modifications to the EU-U.S. Safe Harbor remains to be seen.

Another key Juncker appointment from a privacy perspective is Günther Oettinger of Germany, who was named commissioner for Digital Economy and Society. In Oettinger's mission letter from Juncker, Oettinger is tasked with a number or privacy related tasks:

- ensuring that developments such as the cloud, the Internet of Things and big data can thrive in Europe;
- developing a plan to make the EU a leader in cybersecurity preparedness and increase the confidentiality of communications; and
- finalizing negotiations on Data Protection Regulation in 2015, and then, depending on the outcome of that legislative process, preparing a reform of the e-Privacy Directive.

These and other appointments by Juncker are likely to shape the debate on privacy in the EU in the coming five-year period.

Return to Table of Contents

Skadden contacts appear on the next page.

SKADDEN CONTACTS

STUART D. LEVI
Partner / New York
212.735.2750
stuart.levi@skadden.com

JESSICA N. COHEN
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

TIMOTHY A. MILLER
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

JAMES S. TALBOT
Counsel / New York
212.735.4133
james.talbot@skadden.com

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