Skadden

Privacy & Cybersecurity Update

White House Issues Executive Order Highlighting Trump Administration's Cybersecurity Plans

The Trump administration has issued an executive order setting forth its plans for assessing the nation's cybersecurity, which includes requests for input from agencies across the federal government.

On May 11, 2017, President Donald Trump signed an executive order titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," (the order) outlining the administration's cybersecurity plans.[1] The order focuses on (a) enhancing the security of federal networks and identifying federal information technology procurement needs; (b) reporting on cybersecurity concerns within U.S. critical infrastructure; and (c) reviewing the nation's overall cybersecurity posture and assessing cybersecurity threats. The order asks for multiple reports on each of these topics with input from more than a dozen different federal agencies. The Trump administration appears ready to use the reports generated to set its cybersecurity priorities for the next four years.

Section 1 of the order states that agency heads will be held accountable for assessing and addressing cybersecurity risks. Within 90 days, each federal agency will be required to use the National Institute of Standards and Technology Cybersecurity Framework to develop and provide a risk management report to the civilian or military agencies in charge of assessing federal agency cybersecurity readiness, as appropriate. The agencies in charge of assessing readiness are then required to review those reports and, within 60 days, provide an assessment of cybersecurity risks and a strategy for adequately protecting executive branch agencies from those risks. The order also addresses federal IT modernization, requiring a study addressing the technical feasibility, cost effectiveness and cybersecurity implications of shifting to a consolidated network architecture, or a cloud services model, for IT delivery.

[1] A copy of the order can be found here.

Section 2 of the order addresses cybersecurity risks to U.S. critical infrastructure. As defined in a February 2013 executive order issued by the Obama administration, critical infrastructure industries include any in which "a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." The Trump order asks a number of national security agencies to assess their existing authorities, consult with critical infrastructure industries and then collectively issue a report within 180 days describing how the federal government can support critical infrastructure in protecting its assets against cybersecurity risks. Separately, the order also requires the government to issue a report on market transparency in sharing risk management practices among critical infrastructure entities.

In addition, several agencies are called upon to issue multiple reports addressing specific cybersecurity concerns associated with individual critical infrastructure industries:

- The departments of Commerce and Homeland Security are tasked with leading a process to promote action against threats to the "internet and communications ecosystem." Notably, in the final version of the order, this phrase expands the scope of potential participants beyond those responsible for "core communications infrastructure," which was the phrase used in the initial draft. The order requires the lead agencies to engage with other federal agencies and appropriate stakeholders in the technology and communications industries to develop a plan and report back to the White House on their preliminary results within 240 days;
- The departments of Energy and Homeland Security are required to consult with other agencies and industry stakeholders to develop an assessment of the U.S. power grid's readiness to respond to a significant cyber incident and report back to the White House within 90 days; and
- The departments of Defense and Homeland Security, along with the Federal Bureau of Investigation (FBI), are required to draft a report on risks to the defense industrial base and submit it to the White House within 90 days.

Finally, Section 3 of the order addresses questions germane to the cybersecurity of the nation as a general matter. In addition to various reports on the development of a trained U.S. cybersecurity workforce, this section requires agencies to develop two reports on the country's position in the international cybersecurity order. The departments of State, Treasury, Defense, Justice, Commerce and Homeland Security, and the Office of the U.S. Trade Representative, in coordination with the Directorate of National Intelligence, are asked to assemble a report on "the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats." Many of the same agencies, along with the FBI, are separately asked to submit reports on their "international cybersecurity priorities" and are collectively asked to develop "an engagement strategy for international cooperation in cybersecurity."

Key Takeaways

- **Companies in critical infrastructure industries can expect more engagement from the U.S. government.** Over the next year, agencies will be seeking input from critical infrastructure industry members generally, and those in the communications, technology, energy and defense industries more specifically. The resulting opportunities for both informal discussion and formal participation in the development of the various reports mandated by the order may allow critical infrastructure companies to influence the direction of federal oversight in their respective industries.
- **Companies that manufacture or trade in information technology and foreign companies that invest in U.S. critical infrastructure should closely watch for the report on "strategic options for deterring adversaries."** The inclusion of the departments of State and Commerce, and the Office of the U.S. Trade Representative, in the team of agencies preparing the report demonstrates the Trump administration's interest in using trade remedies to address cybersecurity concerns. The Trump administration recently initiated the first action since 2001[2] under Section 232 of the Trade Expansion Act of 1962, which permits investigation of trade-related threats to national security. Moreover, the overall membership of the authoring agencies group tracks the membership of the Committee on Foreign Investment in the United States (CFIUS), which reviews individual foreign investments into the U.S. for any national security risks they present. The strategic options report may serve as a mission statement for CFIUS and trade agencies determined to use their authority to more aggressively pursue trade practices and foreign acquisitions that may be viewed as adding cybersecurity risk.
- **The report on "international cybersecurity priorities" may serve as an early indication as to how the Trump administration will address U.S.-EU information-sharing and privacy concerns.** Over the last few years, tensions have developed between United States and EU privacy regulators regarding how U.S.-based internet companies collect and use personal data of European citizens. During the Obama administration,

[2] See our recent mailing on this action here.

the U.S. and EU worked to develop agreements, including the Privacy Shield and revisions to the current international scheme of Mutual Legal Assistance Treaties, to address both sides' concerns. However, the Trump administration has not articulated a definitive position on these issues. The international priorities report may shed light on the current administration's views.

Return to Table of Contents

Acting FTC Chairwoman Speaks on Cybersecurity Substantial Injury Definition

Maureen K. Ohlhausen recently made remarks suggesting that the FTC may expand the definition of substantial injury to consumers in cybersecurity-related incidents.

At a recent cybersecurity law event at Georgetown University, Maureen K. Ohlhausen, the acting chair of the FTC, stated that the agency will focus on the definition of substantial injury to consumers that can give rise to enforcement actions under Section 5 of the FTC Act, which provides the FTC with jurisdiction to regulate cybersecurity and consumer privacy. Ohlhausen's focus on defining substantial injury has been a common theme throughout her public comments as chairwoman, and she has been hesitant to regulate in areas where she views harm to consumers as hypothetical. In recent interviews, Ohlhausen has stressed that regulators should tread carefully and has advocated for a less expansive and more transparent interpretation of the FTC's authority under Section 5 of the FTC Act.

Despite this hesitation to expand the regulatory authority of the FTC, her remarks at Georgetown signaled a potential broadening of the types of consumer harms that would qualify as substantial injury. In addition to direct financial harm to consumers, which the FTC has focused on in past, Ohlhausen said that harms such as health and safety risks arising from the sharing of real-time location data could threaten consumers' physical safety and thus constitute a substantial injury. Ohlhausen also pointed to disclosure of sensitive medical information as having the potential to cause substantial injury. The definition of substantial injury is still uncertain, with Ohlhausen saying that "we need to think about this more fully," while also noting that work at the FTC on these issues is ongoing, particularly as it relates to the evolving internet of things and the risks posed by such technology.

Key Takeaways

Acting Chairwoman Ohlhausen's comments at Georgetown suggest that while the FTC may take a more conservative approach to regulation in the privacy and cybersecurity space going forward, the agency may broaden its definition of substantial harm to consumers to include scenarios beyond direct financial harm.

Return to Table of Contents

Target Reaches Settlement with State Attorneys General Regarding Data Breach

Target Corporation has reached an agreement with 47 state attorneys general to settle claims related to its massive 2013 data breach. The agreement includes payment by Target of approximately $18.5 million in settlement fees, as well as Target's commitment to take certain steps to improve its cybersecurity.

Target Corporation has entered into a settlement agreement[3] with the attorneys general of 47 states,[4] as well as the District of Columbia, to settle claims arising out of the 2013 data breach in which computer hackers stole credit and debit card information from approximately 110 million Target customers by installing malware on Target's computer servers. In what has been described by regulators as the largest multistate data breach settlement ever reached, Target has agreed to pay approximately $18.5 million in settlement fees and to take specific steps to improve its cybersecurity. Those steps, summarized below, have been described by Illinois Attorney General Lisa Madigan as setting the industry standard for protecting consumers' information from data breaches going forward.

As part of the settlement, Target commits to do the following:

- within 180 days following the date of the settlement, the company must establish a comprehensive information security program, which must:
  - include administrative, technical and physical safeguards appropriate to the size of Target's operations, the nature of its activities and the sensitivity of the personally identifiable information that it collects;

[3] A copy of the settlement agreement can be found here

[4] California is negotiating its own settlement with Target that is expected to be the same in substance as the settlement agreement, but also will include appropriate changes in form to comply with California law and, accordingly, California has been counted among the 47 states.

  - be supported by appropriate resources; and
  - include steps to handle security breaches involving personally identifiable information;
- employ an experienced cybersecurity executive who is responsible for overseeing the information security program and advising the CEO and the board of directors on the security risks faced by Target and the security implications of the company's decisions;
- develop written risk-based policies and procedures for auditing vendor compliance with the information security program;
- make reasonable efforts to maintain and support the software on its networks;
- maintain protocols to encrypt certain cardholder data;
- scan and map the connections between the portion of its network that processes and stores card authentication data (Cardholder Data Environment) and separate it from rest of its network;
- implement a penetration testing program;
- implement controls to manage access to individual accounts, service accounts and vendor accounts, including strong passwords and password-rotation policies, and two-factor authentication;
- restrict or disable unnecessary network programs that provide access to the Cardholder Data Environment;
- implement a file integrity monitoring solution to notify personnel of unauthorized modifications to critical applications within the Cardholder Data Environment;
- implement controls designed to detect the execution of unauthorized applications within its point-of-sale terminals and servers;
- implement controls to manage the access of any device attempting to connect to the Cardholder Data Environment, and to monitor and log network activity;
- develop policies and procedures to manage and document changes to network systems;
- maintain separation of development and production environments;
- manage the review and, where appropriate, adoption of improved industry-accepted payment card security technologies, such as chip-and-PIN technology; and
- encrypt payment card information throughout the course of retail transactions at retail locations.

Target is required to obtain an information security assessment and report from a qualified third party within one year following the date of the settlement. The report must specify the safeguards implemented by Target and explain the extent to which such safeguards are appropriate in light of Target's operations.

Key Takeaways

The list of steps Target has agreed to take provides a useful cybersecurity checklist for companies, although we would caution against fully relying on this list as the "industry standard," particularly given how quickly the area of cybersecurity protection and preparedness is evolving.

Return to Table of Contents

T-Mobile Denied Access to Data Breach Report Prepared by IT Consultant

In a class action brought by T-Mobile customers against Experian in the wake of a data breach, the U.S. District Court for the Central District of California denied plaintiffs access to a report prepared by a third-party forensics consultant because the law firm representing Experian, rather than Experian itself, commissioned the report in anticipation of litigation.

In September 2015, hackers accessed the IT systems of Experian Information Solutions Inc. (Experian) and stole the personally identifiable information of approximately 15 million T-Mobile USA Inc. (T-Mobile) customers on whom T-Mobile had run credit checks with Experian. The information included customers' names, addresses, social security numbers, birthdays, driver's license ID numbers, military ID numbers and passport numbers. Following discovery of the data breach, Experian immediately hired the law firm Jones Day. Jones Day then hired Mandiant, a third-party information technology forensics consultant, to investigate the breach. Multiple class actions filed on behalf of consumers whose personally identifiable information was stolen

in the breach were consolidated in the U.S. District Court for the Central District of California, and the plaintiffs sought to compel discovery of the report prepared by Mandiant following its investigation. The court denied the motion to compel.[5]

The court ruled that the report was protected by the work product doctrine because it had been ordered by and prepared for Jones Day, rather than Experian itself, in anticipation of litigation.[6] The court found that the facts supported Experian's contention that Mandiant was retained by Jones Day for the sole purpose of helping to prepare a defense to the complaints that would inevitably be filed as a result of the data breach, rather than simply to aid Experian's own internal investigation of the breach. The court found it persuasive that a full draft of the report was provided only to Jones Day and not to Experian's incident response team, and that the report would not have been prepared with the same content and in the same form had Jones Day not been instructing Mandiant.

Key Takeaways

In general, a company's security incident response plan should call for the prompt engagement of counsel, who can then assist in involving other third-party consultants in a manner designed to preserve protections such as the work product doctrine or attorney-client privilege. Whether these protections attach in all cases is highly dependent on the facts of a particular scenario, however, as this ruling demonstrates, retaining third-party consultants through and with the advice of counsel following a data security incident can yield benefits in any ensuing litigation.

Return to Table of Contents

Federal Court Finds System Coding Error Not Covered Under Crime Insurance Policy

A U.S. district court recently held that a prepaid debit card processing company is not covered by its crime insurance policy's computer fraud coverage following a coding error in the company's redemption processing system.

A recent decision from the U.S. District Court for the Northern District of Georgia underscores the need for businesses to evaluate the adequacy of their insurance coverage for potential cyber-related losses stemming from weaknesses or errors in their information technology platforms. In *InComm Holdings, Inc., et al. v. Great American Insurance Company*,[7] the court held that InComm Holdings, Inc. (InComm), a prepaid debit card processing company, was not covered under its crime insurance policy for a loss in excess of $11 million that it sustained when cyber criminals exploited a coding error in InComm's Interactive Voice Response (IVR) system to carry out a fraudulent redemption scheme.

Background

InComm's IVR system is an automated technology that allows prepaid debit card holders to interact with a computer through telephone touch-tone and voice commands to load funds on to prepaid debit cards issued by third-party banks. In order to load funds on to a debit card, the cardholder first must purchase a "chit" from a retailer in the amount that he or she wishes to add to the card. After purchasing a chit, the cardholder would then call InComm's IVR system to redeem the value. Once the chit is redeemed via the IVR system, the chit becomes inactive and InComm transfers funds equal to the value of the chit to the issuing bank.

In May 2014, InComm learned that cyber criminals, without hacking the system, were able to exploit a "code error" in the IVR system that allowed cardholders to redeem single chits multiple times, thereby obtaining more credit than was purchased. The cyber criminals carried out the fraudulent redemption scheme by submitting multiple simultaneous redemption requests for single chits to InComm's IVR system, which the company said resulted in more than 25,000 duplicate redemptions and a loss in excess of $11 million.

Shortly thereafter, InComm submitted a claim for its loss to Great American Insurance Company (Great American), which insured InComm at the time of the loss under a crime insurance policy providing coverage for losses resulting from computer fraud. Great American denied coverage for the claim, concluding that the loss did not fall within the policy's computer fraud coverage.

[5] A copy of the Order Denying Motion to Compel Production of Documents can be found here.

[6] Because the court found that the report was protected by the work product doctrine, it did not analyze whether it also would be protected by the attorney-client privilege.

[7] No. 1:15-CV-2671-WSD, 2017 WL 1021749 (N.D. Ga. Mar. 16, 2017). A copy of the opinion can be found here.

The Court's Decision

InComm argued that its loss was insured by the policy's computer fraud provision, which provided coverage for "loss of … money … resulting directly from the use of any computer to fraudulently cause a transfer of that [money] from inside the premises" to a person or place "outside those premises." In InComm's view, because the IVR system was used to fraudulently redeem chits, the "use of any computer" requirement was satisfied.

The court disagreed and sided with Great American, holding that InComm's loss was not covered by the policy. The court found that adopting InComm's reading of the policy "would unreasonably expand the scope of the Computer Fraud Provision, which limits coverage to 'computer fraud.'" The court reasoned that while the cardholders used telephones to provide responses to prompts from an InComm-operated computer connected to the IVR system, there was no evidence that the cardholders realized that their telephone calls resulted in interaction with a computer. "That the cardholders' use of telephones ultimately led InComm's computer to process multiple chit redemptions does not establish that InComm's loss resulted from the cardholders' 'use of a computer,'" the court opined.

The court further held that even if it was to be assumed that a computer was "used" to perpetrate the fraudulent redemption scheme, InComm still would not be entitled to coverage under the policy's computer fraud provision because InComm's loss did not directly result from the alleged computer use. This was the case, in the court's view, because InComm's loss "occurred only after InComm wired money to [the cardholder's bank], after the cardholder used his card to pay for a transaction, and after [the bank] paid the seller for the cardholder's transaction."

Key Takeaways

The *InComm* decision serves as an important reminder for policyholders to assess their coverage for cyber risks, particularly regarding those that rely on information technology platforms for key business operations, as infrastructure weaknesses and programming errors in such platforms have the potential to cause costly cyber incidents that are not necessarily covered by their existing policies.

Return to Table of Contents

UK Likely to Retain EU Data Protection Laws After Brexit

The United Kingdom appears likely to retain EU data protection laws following Brexit based on the government's announced plan to convert most EU laws into U.K. laws through an omnibus bill. Key questions remain, however, as to how data transfers will be handled if the EU and U.K. laws diverge over time.

Among the many questions surrounding the United Kingdom's exit from the European Union was that of the fate of EU data protection laws in a post-Brexit U.K., including the soon-to-be-enforced General Data Protection Directive (GDPR). However, at the end of March 2017, the British government released a white paper announcing its plan to retain all existing EU laws immediately following the U.K.'s withdrawal from the EU.[8] This plan should provide companies that collect data from the U.K. with some clarity regarding the laws that will apply to those actions, though many details remain unresolved.

The Great Repeal Bill

Before the U.K. leaves the EU, the British government intends to pass a "Great Repeal Bill," which will simultaneously (a) exit the U.K. from the EU, (b) convert all EU laws at the time into U.K. laws, and (c) allow the government to amend EU laws to address issues such as references to EU bodies and other technical matters.

Although the government has not commented on EU data protection laws specifically, so far it seems likely that these laws will be included in the Great Repeal Bill's scope. Elizabeth Denham, the newly appointed head of the U.K. Information Commissioner's Office, has said the U.K. should retain EU laws, stating that she doesn't "think Brexit should mean Brexit when it comes to standards of data protection."[9]

Denham further noted that, were the U.K. not to retain the EU's data protection laws, it would put data sharing between the U.K. and the EU at risk, as the EU only allows personal information to be exported from the EU to countries that, in the EU's view, offer adequate levels of protection for personal data. As Denham noted, "In order for British businesses to share information and provide services for EU consumers, the law has to be equivalent."

[8] The white paper is available here.

[9] "Commissioner: UK 'must avoid data protection Brexit.'"

Impact on the GDPR

The GDPR is set to come into effect in May 2018, which means it will become law before the U.K. leaves the EU and therefore likely will be covered by the Great Repeal Bill. The implementation and interpretation of the GDPR could diverge fairly quickly, however, as U.K. data protection authorities will be able to act independently of EU-wide organizations, such as the EU's Article 29 Working Group, and will not be subject to rulings of EU courts interpreting the GDPR's requirements.

Impact on the Privacy Shield

It remains unclear how the EU-US Privacy Shield, which allows data to be transferred from the EU to those U.S. companies that self-certify to the Privacy Shield, will be addressed post-Brexit. Since this a negotiated agreement, it likely would not be included in the Great Repeal Bill. However, we anticipate that the U.K. would enter into its own parallel agreement, much as Switzerland has done with respect to the Privacy Shield. This would depend, of course, on the Privacy Shield remaining intact (see below for a discussion of some current challenges to the Privacy Shield). If the Privacy Shield is renegotiated in the future, it will be interesting to see if the U.K. enters into its own separate negotiations or follows the lead of the EU.

Key Takeaways

The British government's stated plan to incorporate all EU laws following Brexit provides some degree of certainty to companies that collect personal data in the U.K. However, the risk of divergent interpretations of these laws between the EU and the U.K. over time will require companies to pay close attention to both jurisdictions.

Return to Table of Contents

SEC Issues Risk Alert Following Massive Global Ransomware Attacks

The Securities and Exchange Commission (SEC) released a risk alert encouraging broker-dealers, investment advisers and investment funds to conduct periodic cyber risk assessments and implement systems upgrades on a timely basis in order to reduce the risk of ransomware attacks.

The Office of Compliance Inspections and Examinations (OCIE), the arm of the SEC charged with monitoring risks and improving compliance among market participants through the agency's National Exam Program, released a cybersecurity risk alert on May 17, 2017, in the wake of the widespread "WannaCry" ransomware attacks that had affected organizations in over 100 countries in the preceding days.[10] The alert highlights certain deficiencies in cybersecurity practices across financial firms (as identified in recent examinations) and identifies risk management considerations in order to encourage market participants to strengthen cybersecurity preparedness across the industry.

In a recent examination of 75 SEC-registered broker-dealers, investment advisers and investment funds, OCIE found shortcomings in certain industry cybersecurity practices. Despite nearly all firms having a process in place for regular system maintenance, OCIE's examination found that:

- 26 percent of investment advisers and funds and 5 percent of broker-dealers did not conduct periodic cyber risk assessments of critical systems;
- 57 percent of investment management firms and 5 percent of broker-dealers did not conduct penetration tests or vulnerability scans of critical systems; and
- 4 percent of investment management firms and 10 percent of broker-dealers had a significant number of high-risk security patches missing important updates.

The OCIE alert uses these results to underscore the importance of testing critical systems for vulnerabilities and implementing system upgrades on a timely basis, noting that the WannaCry ransomware has been effective largely due to companies' lack of speed in applying available security patches to the Microsoft systems that were targeted in the attack.

In light of the WannaCry attacks in particular, the alert encourages broker-dealers and investment management firms to evaluate whether they have properly and timely installed applicable patches for affected Windows operating systems, and to review an alert drafted by the U.S. Department of Homeland Security's Computer Emergency Readiness Team[11] that provides technical analysis of the WannaCry ransomware. The alert also recommends prevention, protection and remediation solutions. More broadly, OCIE encourages firms to review periodic guidance and other resources provided by OCIE, the SEC's Division

[10] A copy of the alert can be found here.

[11] The U.S. Department of Homeland Security/U.S. Computer Emergency Readiness Team (US-CERT), Alert (TA17-132A), *Indicators Associated with WannaCry Ransomware* (May 12, 2017, last revised May 19, 2017), can be found here.

of Investment Management and FINRA[12] in order to fortify cybersecurity programs. By developing appropriate planning, increasing rapid response capabilities and strengthening cybersecurity preparedness, OCIE asserts that companies will be better suited to prevent and mitigate the impact of cybersecurity attacks on investors and clients.

Key Takeaways

Companies that are subject to regulation by the SEC should confirm that the Microsoft patches identified in the OCIE alert have been implemented on their critical systems and have a program in place to ensure that future patches are promptly implemented following release.

Return to Table of Contents

District Court Judge Dismisses Data Breach Lawsuit Against Midwest Supermarket Chain

The U.S. District Court for the Southern District of Illinois dismissed a lawsuit brought by a group of banks and credit unions against a supermarket chain in connection with a data breach that occurred before the "data breach boom," finding that the supermarket had not violated either statutory or common law duties with respect to data security.

In *Community Bank of Trenton et al. v. Schnuck Markets Inc.*, the U.S. District Court for the Southern District of Illinois dismissed a lawsuit brought by a group of banks and credit unions against supermarket chain Schnuck Markets (Schnucks) in connection with a data breach it suffered in 2012 and 2013.[13] In dismissing the suit, the district court judge emphasized that there were no allegations that Schnucks ignored warnings about its data security and that the breach "took place during what seemed to be the boom of data breach activity, at a time when many retailers were caught either unaware or unluckily in the cross-hairs of cybercrime."

Background

The lawsuit stemmed from the alleged compromise of unencrypted data for 2.4 million credit and debit cards that were used by customers at 79 Schnucks stores from December 1, 2012, through March 30, 2013. The plaintiffs claimed Schnucks first learned of the possible breach on March 14, 2013, when it received reports of fraudulent card use. Five days later, it retained a forensic investigation firm to examine the issue. According to the plaintiffs, the firm identified the breach on March 20, 2013, but Schnucks did not inform the public until March 30, 2013.

Three payment card issuers, on behalf of themselves and other similarly situated plaintiffs, first filed suit against Schnucks in October 2015. After the court dismissed the initial complaint in September 2016, the plaintiffs refiled in October 2016, alleging violations of the Illinois Consumer Fraud Act, as well as other Missouri and Illinois common law negligence and contract claims.

The Court's Ruling

The district court dismissed all of the plaintiffs' claims, finding that the plaintiffs failed to plead facts that suggested Schnucks had violated a duty to safeguard credit card data. The court specifically rejected the plaintiffs' reliance on the Home Depot[14] and Target[15] data breach cases, both of which survived motions to dismiss. "The facts in the record suggest that Home Depot's data security conduct in the lead-up to their breach was egregious and intentional — Home Depot on numerous occasions ignored warning signs of poor data security, and even went so far as to fire tech employees who tried to alert the company to the risks of the poor data security measures," the court noted. "Such alarming conduct," the court further explained, "certainly weighed heavily on the Northern District of Georgia when deciding whether or not to let a negligence claim proceed." Regarding the *Target* case, the court observed that the duty at issue in that case arose from a special Minnesota statute, which had no analogue in Missouri law, explaining that "in the absence of such legislation, this court declines to *sua sponte* create a duty where the Missouri government has declined to do so."

[12] *See, e.g.*, Division of Investment Management, *IM Guidance Update: Cybersecurity Guidance* (April 2015); *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015); *OCIE's 2015 Cybersecurity Examination Initiative* (Sept. 15, 2015); FINRA *Cybersecurity*.

[13] The opinion and order may be found here.

[14] *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016).

[15] *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304 (D. Minn. 2014).

The plaintiffs also brought implied and third-party beneficiary contract claims, relying on agreements between Schnucks and card issuers Visa and MasterCard that required Schnucks to maintain proper data security. The court rejected those claims as well, ruling that those contracts did not "expressly or impliedly" give the plaintiffs contractual rights. The court also did not find support for the plaintiffs' claim "that they were intended to directly enforce or otherwise control the contractual relationship between the merchant and the card processing network."

Finally, the court dismissed the Illinois Consumer Fraud Act claims, noting that Schnucks had not touted its data security or "lur[ed] customers into the store on the premise that it practiced better data security." The court also emphasized that, "[u]nlike Home Depot's conduct of skirting warnings and firing employees, [Schnucks] retained a firm to investigate a potential breach" soon after learning of it.

The fact that the Schnucks data breach took place in early 2013 (before the prominently publicized data breaches at Target and Home Depot) also played a role in the court's ruling that Schnucks adequately monitored its data security. The court cautioned, however, that "[i]n the wake of the data breach boom, it seems fair to say that retailers will have to act more prudently, but at the time that this breach occurred the law did not contemplate harms of the kind that emerged."

Key Takeaways

The ruling highlights the ways in which a company can help minimize its litigation exposure from a data breach. In dismissing the lawsuit, the court found it significant that Schnucks promptly retained a forensics investigator in the wake of the breach, that it had no track record of ignoring data security problems and that it had not exaggerated the strength of its data security. It remains to be seen, however, whether the court's suggestion that companies should act more prudently following the "data breach boom" of 2013 and 2014 will result in stricter standards being applied by the court going forward.

Return to Table of Contents

Second Circuit Rules Plaintiffs in Data Breach Lawsuits Must Show Concrete Injuries

The Second Circuit affirmed the dismissal of a credit card data breach class action for lack of standing.

In *Whalen v. Michael's Stores, Inc.*, the U.S. Court of Appeals for the Second Circuit affirmed the dismissal of a data breach class action lawsuit against Michaels Stores Inc. (Michaels), stating that the lead plaintiff failed to show that she suffered any actual injury and thus lacked Article III standing.[16] The Second Circuit's decision is part of a growing trend in which plaintiffs have had difficulty establishing standing in data breach cases.

The Second Circuit relied on the Supreme Court case *Clapper v. Amnesty*, which reiterated the long-standing judicial requirement that a plaintiff must allege an injury that is "concrete, particularized, and actual or imminent" to have standing to bring a lawsuit.[17] The Second Circuit explained that the plaintiff failed to show that she suffered, or was likely to suffer, an injury. The plaintiff's complaint described two attempted fraudulent credit card charges, however, neither was successful. Consequently, the court found that these attempts did not constitute an "injury" to the plaintiff sufficient to confer standing. Additionally, the court emphasized that the plaintiff could not possibly face a threat of future fraud, as her stolen credit card was cancelled after the breach and no other personally identifiable information was alleged to have been compromised by the breach.

The court distinguished the *Whalen* case from a 2016 Sixth Circuit case, in which the plaintiffs did establish standing in a lawsuit against Nationwide Mutual Insurance Company. In that case, a data breach could have compromised names, dates of birth, Social Security numbers and drivers' license numbers. According to the Sixth Circuit, although it was not certain that the plaintiffs would suffer an injury as a result of the theft of their data, there was a substantial risk of harm such that incurring mitigation costs was reasonable.[18]

[16] See No. 16-260 (L), 2017 WL 1556116, at *2 (2d Cir. May 2, 2017). A copy of the opinion can be found here.

[17] *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 133 S. Ct. 1138, 1140, 185 L. Ed. 2d 264 (2013).

[18] *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016).

In contrast, in the *Whalen* case, the Second Circuit noted that the plaintiff's risk of future injury was not a concrete threat because none of her other personally identifiable information had been stolen. In addition, the plaintiff did not provide particularized information regarding the time or money she spent monitoring her credit. Instead, her complaint "alleges only that consumers must expend considerable time on credit monitoring and that she and the Class suffered additional damages based on the opportunity cost and value of time." The court found these allegations too vague and insufficient to establish standing.

Key Takeaways

The Second Circuit's decision reflects the continuing difficulty plaintiffs are facing when alleging speculative or future harm in data breach cases. Companies that suffer data breaches and subsequent litigation should carefully assess whether the complaints filed against them plead actual harm as a result of the breach, or at least plead a "substantial risk that the harm will occur." This case, together with other recent cases, suggest that standing will continue to be a key issue in privacy litigation.

Return to Table of Contents

CNN Wins Privacy Battle Over Mobile App in the Eleventh Circuit

The U.S. Court of Appeals for the Eleventh Circuit ruled that a man who had downloaded the free CNN app to his mobile phone was not a subscriber to CNN for purposes of the Video Privacy Protection Act (VPPA), even though he also had a cable television subscription that included content from CNN.

In *Perry v. Cable News Network, Inc.*, the U.S. Court of Appeals for the Eleventh Circuit held that Ryan Perry, a consumer who used a free CNN app on his phone, is not protected as a "subscriber" under the VPPA and thus is not able to make a claim against CNN for sharing his personal information with a third party.[19] This holding may make it easier for the providers of mobile apps to avoid such claims, but the fact that the court did not bar the action on standing grounds may leave opportunities for future litigation under the VPPA.

Background

Perry downloaded CNN's free app in 2013. He was not required to create a separate user name and password to access the app; rather, he used an ID number provided to him by his cable television provider. Perry used the app and such ID to access content that was freely available to all users of the app, as well as certain content that was available only to those users with cable television subscriptions that included CNN. The VPPA prohibits a provider of audio/visual materials from disclosing a customer's personally identifiable information without consent.[20] In a putative class action, Perry alleged that CNN violated the VPPA because the app disclosed users' viewing activity and mobile device MAC addresses to a third-party data analytics company without users' consent.

The Court's Decision

The court first applied the Supreme Court's decision in *Spokeo* in a standing analysis and found that the alleged procedural violation in this case was sufficient to constitute an injury-in-fact. This ruling provides a liberal reading of the *Spokeo* decision, which held that bare procedural violations divorced from any concrete harm are not enough to constitute standing. The Eleventh Circuit found that the "structure and purpose of the VPPA supports the conclusion that it provides actionable rights." In finding as such, the court partially relied on the fact that in creating a cause of action for an invasion of privacy, the VPPA addresses "a harm that has traditionally been regarded as providing a basis for a lawsuit in English and American courts," while also observing that Supreme Court precedent points to a privacy interest in "preventing disclosure of personal information." Accordingly, the court concluded that a violation of the VPPA, by itself, is a harm sufficient to confer standing.

Though Perry cleared the hurdle of standing in this case, the court did not agree that he suffered an injury as a "subscriber" that would entitle him to bring a claim under the VPPA. According to the court, Perry was not a subscriber because he had not demonstrated an "ongoing commitment or relationship with CNN." In making this ruling, the court relied on *Ellis v. Cartoon Network, Inc.*,[21] which held that a user of a free mobile app is not necessarily a "subscriber" for purposes of the VPPA. The court pointed to a dearth of contacts between Perry and CNN, as evidenced by no direct payments, a lack of a user profile and other factors to support its conclusion that *Ellis* was controlling

[19] A copy of the decision is available here.

[20] The text of the VPPA is available here.

[21] A copy of the decision can be found here.

in this case. The court was not persuaded by the fact that Perry is a cable television subscriber and CNN's inclusion in his television bundle allowed him to access certain functionality and features on the app. The court found that this arrangement only showed a commitment to his cable television provider, not CNN, stating, "the ephemeral investment and commitment associated with Perry's downloading of the CNN App on his mobile device, even with the fact that he has a separate cable subscription that includes CNN content, is simply not enough to consider him a 'subscriber' under *Ellis*." The court distinguished the First Circuit decision in *Yershov v. Gannett Satellite Information Network, Inc.*,[22] in which the First Circuit found that the end user of an app provided by *USA Today* was a subscriber of *USA Today* for purposes of the VPPA, by noting that in *Yershov* the plaintiff had provided his mobile device identification number and GPS location to *USA Today*, which in that case was sufficient to establish an ongoing "subscriber" relationship.

Key Takeaways

Though this case provides a clearer path to establishing Article III standing for violations of the VPPA, it also makes it more difficult for mobile app users to bring successful actions under this statute in the Eleventh Circuit if they simply downloaded a free app without creating a user account or providing specific information requested by the app. It remains to be seen how this case will shape the law under other privacy-related statutes and in other circuits, although given the prevalence of mobile apps corresponding to subscription-based services in other media, we should expect to see more litigation in this area in the future.

Return to Table of Contents

[22] A copy of the decision is available here.

Contacts in the Cybersecurity and Privacy Group

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

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

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

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

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

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

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

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

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

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

William Ridgway
Counsel / Chicago
312.407.0449
william.ridgway@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