Skadden

Privacy & Cybersecurity Update

FCC Stays Implementation of New Privacy Rules for ISPs

As many suspected, after the election of President Trump, the FCC has stayed implementing the new consumer privacy rules that were announced in October 2016 and were scheduled to go into effect on March 2, 2017.

The first step has been taken in what many anticipate will be a curtailing of consumer privacy protections under the Trump administration. On March 1, 2017, the Federal Communications Commission (FCC) announced that it stayed the implementation of new internet service provider (ISP) privacy rules that were announced in October 2016. As part of those rules, ISPs were required to obtain explicit "opt-in" consent before collecting a wide range of what was deemed "sensitive information," inform consumers as to what data the ISP would collect and allow consumers to opt out of most ISP information collection. While "sensitive" data included categories that traditionally are considered sensitive, such as health and financial information and information concerning children, it also included a number of categories that are the lynchpin of targeted advertising and a key revenue source for ISPs, including web browsing and app usage history.

When the rules were announced, many questioned not only the substance of the law, but also the concept of the FCC announcing privacy rules that were more restrictive on ISPs than privacy rules imposed by other regulators, such as the Federal Trade Commission (FTC), on other types of providers. Therefore, it is not surprising that the Trump administration, as part of its focus on decreased regulation, targeted the FCC privacy rule.

In a joint statement, Acting FTC Chairwoman Maureen K. Ohlhausen and FCC Chairman Ajit Pai stated they had disagreed with "the FCC's unilateral decision in 2015 to strip the FTC of its authority over broadband providers' privacy and data security practices, removing an effective cop from the beat," and that privacy jurisdiction should be returned to the FTC. Ohlhausen and Pai pledged "to establish a technology-neutral privacy framework for the online world," which they said would be in "the best interests of consumers and has a long track record of success."

Three Recent Cases Question Plaintiffs' Standing in Privacy Actions

A series of recent cases demonstrates the challenges that plaintiffs are facing in establishing standing in privacy cases given the speculative nature of the harm that is often at issue in such cases. We summarize each case and their common themes below.

In re Target Corp. Customer Data Security Breach Litigation

Background

The case stems from Target's 2013 high-profile data breach, which compromised the financial and personal information of up to 110 million consumers.[1] In August 2014, 112 consumer representatives filed a class action lawsuit against Target in the District of Minnesota. After the case survived a motion to dismiss, the parties agreed to settle on a class basis. The district court preliminarily certified a settlement class, without receiving any objections, in which class was defined to encompass "all persons in the United States whose credit or debit card information and/or whose personal information was compromised" as a result of the breach. Under the terms of the settlement, Target agreed to establish a $10 million settlement fund, which would be distributed first to class members with documented losses up to $10,000 per claimant, and the remainder to those with undocumented losses, amounting to an estimated payment of $40 for those claimants. Class members who suffered no loss from the breach would receive nothing from the settlement fund, but still would be bound under the settlement to release Target from liability for any claims should they arise in the future. Target also agreed to permit an attorney fee award of up to $6.75 million and to implement improvements to its data security program, such as appointing a chief information security officer, developing safeguards to control identifiable security risks and providing security training to employees.[2]

In November 2015, the district court, without revisiting the issue of class certification, approved the class action settlement over the objections of a small number of class members, including Leif Olson, who was represented by the Center for Class Action Fairness. Olson, who appealed the certification, complained that he and other members of the class who had suffered no damage as a result of the data breach, but might in the future, stood to receive nothing under the settlement but were nonetheless required to release future claims. According to Olson, the requirements of Federal Rule of Civil Procedure 23(a) were not met because this so-called "zero-recovery subclass" could not be adequately represented by class representatives who received compensation under the settlement.

Decision

The Eighth Circuit ruled that the district court abused its discretion by failing to analyze Olson's objections in the course of approving the class settlement, requiring the settlement to be reconsidered on remand. As the Eighth Circuit observed, the district court "failed its continuous duty to evaluate certification throughout the litigation" by refusing to reconsider the issue of class certification in its final order.

Next Steps

The case now returns to the district court, where the court must "conduct and articulate a rigorous analysis of Rule 23(a)'s certification prerequisites as applied to this case, which must expressly evaluate the arguments raised in Olson's objection." The Eighth Circuit further instructed the district court to consider: (1) "whether an interclass conflict exists when class members who cannot claim money from a settlement fund are represented by class members who can"; (2) "if there is a conflict, whether it prevents the class representatives from fairly and adequately protecting the interests of the class members"; and (3) "if the class is conflicted, whether the conflict is 'fundamental' and requires certification of one or more subclasses with independent representation."

Practical Implications

This decision leaves open the question of class certification in consumer data breach cases where the class includes those who have suffered no damages. Many courts have wrestled with whether plaintiffs who have suffered no pecuniary loss from a data breach have standing to sue, particularly in the wake of the Supreme Court's decisions in *Clapper vs. Amnesty International*, which rejected a theory of "future injury" as too speculative, and *Spokeo v. Robins*, which urged courts to consider the "concreteness" of an injury for standing.

This decision also underscores the fact that defendants in a data breach class action may have trouble grouping together in a settlement those who already have suffered harm with those who argue they may suffer harm in the future, especially given that some courts have been sympathetic to the "future harm" theory argument. For example, in *Lewert v. P.F. Chang's China Bistro, Inc.*, the Seventh Circuit ruled that customers affected by a data breach involving credit card information have standing to sue,

[1] See In re Target Corp. Customer Data Sec. Breach Litig., No. 15-3909, — F.3d —, 2017 WL 429261 (8th Cir. Feb. 1, 2017) available here.

[2] Further background on this case can be found in our March 2015 *Privacy & Cybersecurity Update* here.

despite not suffering any actual out-of-pocket financial harm,[3] and in *Galaria v. Nationwide Mutual Insurance Co.*, the Sixth Circuit held that plaintiffs whose personal information had been obtained by hackers had standing to sue based on the risk of future identity theft.[4] Requiring a subset of class members to release unknown future claims without compensation is likely to draw objections and potentially lead to further litigation, as it did here. A company that seeks to settle a data breach class action will need to take into account the admonition from the Eighth Circuit in this case.

Vigil et al. v. Take-Two Interactive Software Inc.

The U.S. District Court for the Southern District of New York, citing *Spokeo*, dismissed a class action in *Vigil et al. v. Take-Two Interactive Software Inc.*, which was brought against Take-Two Interactive Software Inc. (Take Two) by brother and sister plaintiffs alleging violations of the Illinois Biometric Information Privacy Act (the BIPA).[5]

Background

Although the BIPA was intended to regulate the use of biometric identifiers as a means to identify people in lieu of passwords, the wording of the statute arguably covers any type of biometric scan. A company collecting biometric identifiers must inform the data subject in writing that the biometric identifier is being collected, provide the data subject with a written policy setting forth a retention schedule for the biometric identifiers and receive a written release from the data subject for such collection. Further, the BIPA prohibits dissemination of the biometric identifiers without written consent of the data subject.[6]

Take Two produces video games, including "NBA 2K15" and "NBA 2K16," that allow users to capture and store 3-D scans of themselves and create their own avatars that they can insert into a game. The plaintiffs, on behalf of thousands of Illinois residents who used the scanning feature of the games, alleged that Take Two's practices of obtaining and storing these 3-D facial scans indefinitely, and making the scans available to other players online, in each case without providing a written retention policy or obtaining the plaintiffs' written consent, constituted violations of the BIPA.

Decision

The court found that although Take Two's actions may have technically violated the BIPA's notice and consent requirements, the violations themselves were not sufficient to grant standing. *Citing Spokeo, Inc. v. Robins*, in which the Supreme Court ruled that a simple statutory violation or "bare procedural violation" divorced from concrete harm does not satisfy the Article III standing requirement of injury-in-fact,[7] the judge stated that, "[t]he purported violations of the BIPA are, at best, marginal, and the plaintiffs lack standing to pursue their claims for the alleged bare procedural violations of the BIPA." The court pointed out that the data gathered by Take Two was used as advertised in order to create unique avatars for use while playing "NBA 2K15" or "NBA 2K16" and were visible only to other players during multi-player gaming. As such, the court ruled that the alleged BIPA violations constituted the type of "bare procedural violations" that Spokeo was meant to exclude, and did not satisfy the harm that the BIPA was intended to curb. The court therefore declined to grant standing in this case.

Beck et al. v. McDonald et al.

On February 6, 2017, the Fourth Circuit affirmed the dismissal of two putative class actions brought by military veterans affected by two separate data breaches, holding that the plaintiffs lacked standing because they did not allege facts showing "certainly impending" harm or a "substantial risk that the harm will occur" as a result of the breaches.

Background and Claim

The plaintiffs in this case were two groups of military veterans who received medical treatment and health care at a Veteran Affairs Center in South Carolina (VA Center). The VA Center suffered two data breaches that compromised the personal information of the two groups of veterans. The first data breach occurred in 2013 when a laptop was stolen, containing unencrypted personal information, including the names, birth dates, last four digits of social security numbers and physical descriptors of approximately 7,400 patients. Internal investigations revealed that the VA Center failed to follow procedures and policies for using non-encrypted laptops to store patient information. The second data breach occurred in 2014, when four boxes of pathology reports were either misplaced or stolen. These reports contained identifying information of more than 2,000 patients, including names, social security numbers and medical diagnoses.

[3] *See Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), which was covered in the April 2016 issue of our *Privacy & Cybersecurity Update* here.

[4] *See Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, — F.3d—, 2016 WL 4728027 (6th Cir. Sep. 12, 2016).

[5] The opinion and order can be found here.

[6] The text of the BIPA may be found here.

[7] See our May 2016 *Privacy & Cybersecurity Update* for coverage of the *Spokeo* case here.

After each breach, the VA Center notified the affected patients and offered one year of free credit monitoring. The plaintiffs filed putative class actions against the VA Center on behalf of the affected patients, alleging in both cases that the VA Center violated various legal duties and federal privacy laws by failing to safeguard patients' personal information. In both actions, the plaintiffs alleged that as a result of the data breaches, they faced an increased likelihood of identity theft and costs for measures to protect themselves against future harm, as well as embarrassment, mental distress and inconvenience. There were no allegations of monetary loss (other than fees spent to monitor credit reports) or actual misuse of the stolen data. In both actions, the district court granted the defendants' motion to dismiss on the basis that plaintiffs' fear of harm from future identify theft was too speculative to confer standing.

Both sets of plaintiffs appealed the district court's rulings that they lacked Article III standing, and the cases were consolidated on appeal.

The Court's Decision

The Fourth Circuit affirmed the district court's rulings, holding that the plaintiffs lacked Article III standing because none of their alleged injuries constituted an injury-in-fact. The panel held that because neither set of plaintiffs pointed to any evidence that information was actually misused or even stolen for the purpose of misuse, the plaintiffs' claim of enhanced risk of future identity theft was too speculative to confer standing.

The Fourth Circuit first held that the plaintiffs failed to plead a "certainly impending injury," noting that the "mere theft of [the laptop and pathology reports], without more, cannot confer Article III standing." The panel acknowledged that in three circuits (the Sixth, Seventh and Ninth), an increased risk of identity theft had been enough to confer standing in certain situations. But the Fourth Circuit noted that in each of those cases, the plaintiffs alleged facts that "push[ed] the threatened injury beyond speculative to sufficiently imminent." Such facts included that the information stolen was targeted for identity theft or that some consumers in the class actually suffered identity theft or other misuse of their information, making the likelihood of identity theft more real for the other class members. No such allegations were present in either of the two complaints at issue. The court held that for the plaintiffs' feared harm to materialize, too many possibilities would have to occur: "that the thief targeted the stolen items for the personal information they contained … [and that] the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities." The Fourth Circuit held that this "attenuated chain" was insufficient to confer standing. The court's decision was supported by the fact that "even after extensive discovery" in the case involving the laptop, the "plaintiffs have uncovered no evidence that any of the stolen information has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information."

Next, the Fourth Circuit held that the plaintiffs failed to establish that a "substantial risk" of future harm was likely to occur as a result of the breaches. The plaintiffs argued that the VA Center's offer of free credit monitoring constituted an admission that the theft of the laptop and loss of reports gave rise to a substantial risk of harm. Disagreeing with a similar Sixth Circuit case, *Galaria et al. v. Nationwide Mut. Ins. Co.*[8], the Fourth Circuit "decline[d] to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals. To adopt such a presumption would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit." In this case, unlike in *Galaria*, there was no evidence that the thieves who stole the laptop had misused or intended to misuse the personally identifiable information stored on the laptop, and, as such, it appears that the theft of the personally identifiable information was merely incidental to the theft of the laptop. Accordingly, the court found the harm in this case was too speculative to confer standing.

Lastly, the Fourth Circuit rejected the plaintiffs' claim that they suffered harm by being forced to enroll in credit monitoring, holding that a "self-imposed harm" cannot confer standing, and affirmed the district court's dismissal of the plaintiffs' injunctive relief claims under the federal privacy laws, holding that past data breaches alone "are not sufficient to confer standing."

Key Takeaways

The decisions in *In re Target Corp.*,*Vigil et al. v. Take-Two Interactive Software Inc.* and *Beck et al. v. McDonald et al.* reflect the continuing difficulty plaintiffs face when alleging speculative or future harm in data breach cases. Companies who 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 pose a "substantial risk that the harm will occur."

These cases suggest that after the court's ruling in *Spokeo*, plaintiffs may have a more difficult time establishing standing in privacy cases in certain jurisdictions. We anticipate that battles over standing will continue to remain a critical juncture in any privacy litigation.

Return to Table of Contents

[8] See *Galaria et al. v. Nationwide Mutual Insurance Co.*, Nos. 15-3386/3387 (6th Cir. Sept. 12, 2016) (unpublished). A copy of the decision is available here.

Third Circuit Rules That Alleged Violations of the Fair Credit Reporting Act Are Sufficient to Show Standing

The Third Circuit ruled in *In re: Horizon Health Care Services Inc.* Data Breach Litigation that the plaintiffs have Article III standing to bring claims under the Fair Credit Reporting Act arising out of the theft of two laptops containing their sensitive personal information.

Background

The case arose out of the November 2013 theft from health insurance provider Horizon Healthcare Services, Inc. (Horizon) of two laptops on which unencrypted sensitive personal information of more than 839,000 Horizon customers was stored. Four named plaintiffs, on behalf of themselves and other Horizon customers whose information also was stored on the laptops, filed suit against Horizon alleging violations of the Fair Credit Reporting Act (FCRA), as well as violations of various state laws. The FCRA seeks to, among other things, protect consumer privacy, and provides that any entity covered by the FCRA that regularly assembles or evaluates consumer credit information for the purpose of furnishing consumer reports to third parties must adopt reasonable procedures to keep such information confidential. The FCRA provides that any covered entity that fails to comply with such requirements with respect to any consumer is liable to such consumer.

Three of the named plaintiffs in *Horizon* did not allege that their identities had been stolen as result of the theft of the laptops, but alleged that the violations of the FCRA with respect to their personal information constituted an injury-in-fact and that they suffered an imminent risk of future identify theft as a result of those violations. The fourth named plaintiff, Mitchell Rindner, alleged that as a result of the theft his 2013 tax refund was stolen through the filing of a fraudulent return and there was an attempted fraudulent use of his credit card. The district court dismissed the complaint for lack of Article III standing on the grounds that the plaintiffs had not suffered a cognizable injury, noting that mere violations of statutory rights were not a sufficient showing of injury, and the risk of future harm was too attenuated.[9] The plaintiffs appealed to the Third Circuit.

[9] See the March 2015 edition of the *Privacy & Cybersecurity Update* for coverage of the district court case here.

The Court's Ruling

The Third Circuit found that even without evidence the plaintiffs' information was used or likely to be used improperly, and the alleged FCRA violations give rise to a *de facto* injury sufficient for Article III standing purposes.[10] Citing *In re Google Inc. Cookie Placement Consumer Privacy Litigation*[11] and *In re Nickelodeon Consumer Privacy Litigation*,[12] in which the Third Circuit recently found that even in the absence of economic loss, mere violations of the Stored Communications Act and the Video Privacy Protection Act conferred Article III standing, the court stated that in including a private right of action in the FCRA, Congress had clearly believed that mere violation of the statute could cause concrete harm to consumers. The court distinguished this case from *Spokeo, Inc. v. Robins*[13] by noting that in that case, the plaintiff had alleged a "mere procedural violation" of the FCRA, while in this case the result of the violation was the very harm that the FCRA seeks to protect against. The Third Circuit vacated the district court's decision and remanded the case.

Key Takeaways

The Third Circuit's decision highlights that, in at least some jurisdictions, the standing requirement set forth in *Spokeo* will not always result in dismissal of a data breach action, particularly where the plaintiffs allege violation of a specific statute.

Return to Table of Contents

Smart TV Privacy Settlement Signals Possible Shift in FTC's Definition of Injury

In a recent settlement of a privacy case, a concurrence by now Acting FTC Chairwoman Maureen K. Ohlhausen suggests the FTC, under the Trump administration, may focus on whether there was substantial injury to consumers when deciding whether to bring privacy actions.

The FTC and the New Jersey Attorney General's Office recently settled a privacy action against Vizio, Inc. regarding the company's practice of gathering television viewing data from certain users of its smart TVs. Particularly noteworthy was the concurrence

[10] See here for a copy of the opinion.

[11] 806 F.3d 125 (3d Cir. 2015).

[12] 827 F.3d 262 (3d Cir. 2016).

[13] See the May 2016 edition of the *Privacy & Cybersecurity Update* here for a summary of *Spokeo*.

written by now Acting FTC Chairwoman Maureen K. Olhausen, in which she questioned the treatment of television viewing data as so-called "sensitive information" and reiterated that the FTC's enforcement actions in the privacy area should be grounded in whether substantial injury to consumers is likely to occur.[14]

As we noted in our January 2017 *Privacy & Cybersecurity Update*, Ohlhausen was designated as the acting chairwoman of the FTC by President Trump in January to replace FTC Chairwoman Edith Ramirez. Throughout her tenure at the FTC, Ohlhausen has critiqued the agency for bringing actions where there was only hypothetical harm to consumers. Ohlhausen has stressed that regulatory enforcers should tread carefully and has advocated for a narrower and more transparent interpretation of the FTC's authority under Section 5 of the FTC Act, which provides the FTC with jurisdiction to regulate cybersecurity and consumer privacy. For example, in response to the FTC's report on the potential dangers of big data, titled "Big Data: A Tool for Inclusion and Exclusion," Ohlhausen issued a separate statement expressing concerns that the report failed to take into account market and economic forces, and was distracted by hypothetical harms.[15]

In her Vizio concurrence, Ohlhausen revisits many of the concerns she raised throughout her tenure as a commissioner. Ohlhausen indicated that the injury finding in the Vizio case "demonstrates the need for the FTC to examine more rigorously what constitutes 'substantial injury' in the context of information about consumers," and she promises to "launch an effort to examine this important issue further." She also wrote that "there may be good policy reasons to consider [television viewing activity] information sensitive," however, she warned that "under our statute, we cannot find a practice unfair based primarily on public policy. Instead, we must determine whether the practice causes substantial injury that is not reasonably avoidable by the consumer and is not outweighed by benefits to competition or consumers." In January of this year, Ohlhausen made a similar promise at the 2017 State of Net Conference, vowing to begin efforts to define substantial harms in keeping with her overall principle of practicing "regulatory humility."

Key Takeaways

The FTC remains a consensus-driven organization, and it is too early to determine how the agency, under Ohlhausen, will evolve with respect to privacy matters. While we expect that consumers' data privacy protections will remain a focal point of the FTC, it is quite possible that the agency will adopt a more business-friendly approach and limit the actions it brings to cases where there is actual, and not hypothetical, harm to consumers.

In addition, the makeup of the FTC will continue to change drastically over the course of this year. With Ohlhausen stepping up as acting FTC chair, Terrell McSweeny is the only remaining Democratic commissioner, with her term expiring in September. By law, the commission is headed by five commissioners who are nominated by the president and confirmed by the Senate. The term for each commissioner, including the chair, is seven years, and no more than three commissioners can be of the same political party. President Trump will have the opportunity to nominate three commissioners, and a fourth by the end of 2017 after McSweeny steps down.

Return to Table of Contents

New York Finalizes Cybersecurity Regulations for Financial Institutions

On March 1, 2017, new cybersecurity guidelines for New York-based financial institutions took effect. Companies will need to consider whether their current practices are in compliance with the new regulations.

New York state has finalized new cybersecurity regulations for banks, insurance companies and other financial services institutions regulated by the New York State Department of Financial Services (DFS), concluding an effort that began in 2014. As we reported in our December 2016 *Privacy & Cybersecurity Update*, the DFS first introduced the proposed regulations in September 2016 and released an updated version in December following an initial 45-day comment period.[16] The updated regulations were then subject to a further 30-day comment period resulting in the final regulations, which are substantially similar to those released in December.[17] The regulations took effect on March 1, 2017. Companies subject to the regulations will have 180 days from the effective date to comply with most of the requirements and will have one year from the effective date to implement reporting by the chief information security officer to the board; provide regular cybersecurity awareness training to all personnel; implement mandatory annual penetration testing, bi-annual vulnera-

[14] The FTC's settlement can be found here.

[15] Visit here for a copy of the statement.

[16] View the September 2016 edition (describing the regulations generally) and December 2016 edition of the *Privacy & Cybersecurity Update*: here and here, respectively.

[17] View the DFS press release here and the final regulation here.

bility assessments and periodic risk assessments; and implement effective controls based on the company's risk assessments.

Furthermore, companies will have 18 months from the effective date to comply with the audit trail procedures, develop a program that addresses the security of both in-house developed applications and externally developed applications, create policies for the disposal of nonpublic information, implement risk-based policies to monitor the activity of authorized users of the company's information systems and implement controls, such as encryption, to protect nonpublic information.

Finally, companies will have two years to implement policies to ensure the security of systems and nonpublic information that are accessible by third-party service providers.

Key Takeaway

Companies subject to the new regulations should consider whether their current practices are in compliance with the new regulations and, if not, develop and implement plans to ensure compliance in accordance with the timelines above.

Return to Table of Contents

Article 29 Working Party Issues Dispute Resolution Procedures for Data Protection Authorities Under EU-US Privacy Shield

The Article 29 Working Party has issued procedural rules that clarify the process by which data protection authorities will resolve data subject complaints under the EU-US Privacy Shield.

On February 20, 2017, the Article 29 Working Party (WP29), an EU advisory body charged with providing expert guidance on data protection issues and promoting uniform application of data protection laws across the EU, issued procedural rules governing the review of data subject complaints by EU data protection authorities (DPAs) under the EU-U.S. Privacy Shield.[18]

To satisfy the requirements of self-certification under the Privacy Shield, U.S. companies must offer — at no cost to data subjects — an independent recourse mechanism to address privacy complaints that the company has been unable to resolve directly with the data subject. In general, companies may satisfy this requirement either through dispute resolution programs developed by private sector organizations, such as the American Arbitration Association or JAMS, or by committing to cooperate and comply with DPAs in reviewing and resolving such complaints. Companies that process human resources data under the Privacy Shield in the context of an employment relationship must use the DPA approach. The WP29 rules expand upon this principle from the Privacy Shield and clarify the process by which a panel of DPAs will be formed and resolve such complaints.

According to the process laid out by WP29, each DPA review panel will be comprised of a "lead DPA," which as a general rule will be the DPA that first received the complaint and two other "co-reviewer" DPAs who have expressed an interest in participating. More than two DPAs may be designated as co-reviewers if other DPAs would like to join the panel and are able to put forward a "specific interest." If fewer than two additional DPAs are interested in reviewing the complaint, the lead DPA must designate co-reviewers as necessary to fill a three-member panel. In designating co-reviewers, the lead DPA should consider (1) where the headquarters or significant subsidiaries of the U.S. company's group are located, (2) where the relevant EU data processing occurs, (3) where most of the applicable EU data transfers take place, (4) where a large number of EU individuals are likely to be affected by the alleged violation, (5) whether any specific DPA holds particular expertise in the area in question and (6) available resources. The WP29 rules state that the identification of the lead DPA and the co-reviewer DPAs should be confirmed within two weeks of receiving the initial complaint.

The DPA that receives the complaint will first confirm that the panel is the competent authority to review the complaint, based on whether or not the company has committed to cooperate with the DPAs as part of its self-certification process or whether it processes HR data under the Privacy Shield. If appropriate, the data subject will be advised to first exhaust the internal complaint processes offered by the company. The lead DPA will inform the company of the substance of the complaint and any other relevant information, and the data subject and the company will each be given an opportunity to comment and provide relevant evidence. While no formal procedure has been established regarding submissions by the parties to the dispute, the WP29 rules state that advice will be issued by the DPA panel only after both sides have had "a reasonable opportunity" to provide input. The panel will aim to reach a consensus on each matter within 60 days, with the lead DPA having the deciding vote in the event that consensus cannot be reached. The panel will then issue binding advice, including remedies if applicable, and the company will have 25 days from delivery of the advice to comply. Where appropriate, results of such DPA panel reviews will be made public.

[18] See here for a copy of the rules.

Compliance with the DPA panel's binding advice is mandatory. Notably, if a company fails to comply in the specified timeframe without providing a "satisfactory explanation for the delay," the lead DPA must refer the matter to the appropriate U.S. agency tasked with overseeing the application of the Privacy Shield to the company at issue. This is typically the Federal Trade Commission or the Department of Transportation. In cases of serious compliance failures, the DPA may notify the Department of Commerce to revoke the company's Privacy Shield certification.

Return to Table of Contents

Harvard Business Review Reveals Corporate Boards Are Not Prioritizing Cybersecurity

A *Harvard Business Review* report shows that many boards of directors are not focused on cybersecurity risks.

A recently published report by the *Harvard Business Review* reveals that corporate boards of directors are less concerned with cybersecurity risks than other threats, such as regulatory and reputational concerns.[19] Only 38 percent of directors reported that they had a high level of concern about cybersecurity, and even fewer said they were prepared for these risks. Additionally, when asked to identify the three biggest challenges to their company, only 8 percent of respondents listed cybersecurity.

The report was the result of a survey of more than 5,000 board members of companies with headquarters in over 60 countries conducted by Harvard Business School and the WomenCorporateDirectors Foundation. The survey revealed that boards lack the processes and expertise they need to analyze and minimize cybersecurity risks. Of the directors surveyed, only 24 percent rated their boards' processes to prevent and handle the aftermath of a potential data breach as "above average" or "excellent." Moreover, the opinions among directors regarding these processes varied by industry. For example, in the IT and telecom sectors, 42 percent of the directors surveyed said their boards had strong cybersecurity processes, while in the health care industry, which is a uniquely vulnerable target for data breaches, 79 percent of directors surveyed said their organizations lack strong cybersecurity processes.

The survey results are troubling given that a data breach can result in enormous financial costs and reputational harm, and is one of the key risks that many companies face today. Therefore, it is crucial that boards are aware of the cybersecurity risks facing their companies and the steps that are being taken to reduce these risks.

Board knowledge of cybersecurity threats and preparedness is a long-standing principle of good corporate practices. For example, the new cybersecurity regulations issued by the New York State Department of Financial Services (DFS) (discussed in this issue) require companies subject to regulation by the DFS to designate a chief information security officer who reports at least annually to the board about the company's cybersecurity program and material cybersecurity risks. In October 2016, the Federal Reserve, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation (FDIC) issued a joint advanced notice of proposed rulemaking that would require a company's board of directors to approve the company's overall cybersecurity strategy and have adequate expertise in cybersecurity so it can provide a credible challenge to management on these issues.[20] Further, the 2015 "A Framework for Cybersecurity" report from the Division of Risk Management Supervision of the FDIC stresses that board and senior management should play a role in understanding cybersecurity and promoting a culture that is aware of these risks across the company.[21] In August 2016, the National Association of Insurance Commissioners Cybersecurity (EX) Task Force released a revised draft of its Insurance Data Security Model Law that requires covered entities to provide written reports to the board regarding the entity's cybersecurity program.[22]

Boards also face the possibility of shareholder lawsuits for decisions they made, or failed to make, regarding cybersecurity preparedness. In the wake of the massive data breaches experienced by Target Corp. in 2013 and Home Depot in 2014, shareholders of each company sued the board, alleging that the directors failed to put sufficient internal controls in place to address the risk of a data breach. While the bar for director liability is high, and the directors ultimately prevailed in each of those cases, substantial time and resources are required to defend these actions.

[19] For the *Harvard Business Review* article summarizing the study, see here.

[20] See the October 2016 issue of our *Privacy & Cybersecurity Update* here.

[21] For more information on the FDIC framework, see the February 2016 *Privacy & Cybersecurity Update* here.

[22] See the August 2016 issue of our *Privacy & Cybersecurity Update* here.

Key Takeaway

Companies should take steps to ensure that their boards are sufficiently aware of cybersecurity threats faced by the company and the measures the company is taking to counter those threats. In addition to the financial and reputational risk to the company posed by a cybersecurity incident, those companies in regulated industries could face regulatory action if their practices do not conform to guidance issued by their regulators.

Return to Table of Contents

US Treasury Announces Stand-Alone Cyber Insurance Policies Are Covered by the Terrorism Risk Insurance Act

The U.S. Treasury announced in a recent publication that stand-alone "cyber liability" insurance policies are covered under the Terrorism Risk Insurance Act, an announcement that may speed growth of the cyber insurance market.

On December 27, 2016, the U.S. Department of the Treasury issued a notice of guidance[23] announcing that stand-alone "cyber liability" insurance policies are included under the Terrorism Risk Insurance Act of 2002, as amended (TRIA). This announcement should provide some level of comfort to insurers and policyholders amid growing concern of cyber terrorism flowing from an increasingly interconnected and digitalized society and may help speed market growth for stand-alone cyber liability policies.

Following the September 11, 2001, terrorist attacks, insurers and reinsurers became reluctant to insure against terrorism risks due to the inability to accurately price and model exposures. Many eventually exited that market, which led to a severe shortage of terrorism risk insurance. In order to stabilize the terrorism risk insurance market and ensure the continued availability of such insurance, Congress passed the TRIA. The TRIA requires participating insurers to "make available" terrorism risk insurance for commercial property and casualty losses resulting from certified acts of terrorism and provides for a federal reinsurance backstop in the event of qualifying terrorist attacks. Enacted in November 2002, the TRIA has been extended three times, most recently in January 2015 under the Obama administration. Absent an extension, the TRIA is scheduled to expire on December 31, 2020.

The TRIA applies to "property and casualty insurance," which is defined by reference to insurance coverage lines listed in a National Association of Insurance Commissioners (NAIC) publication used by state insurance regulators for reporting purposes. Prior to January 1, 2016, the NAIC publication did not list cyber liability insurance as a coverage line, and therefore cyber liability insurance policies were not covered under the TRIA. As of January 1, 2016, however, the NAIC added "cyber liability" insurance to the publication as a sub-line of "other liability" insurance, defined in relevant part as follows:

> Stand-alone comprehensive coverage for liability arising out of claims related to unauthorized access to or use of personally identifiable or sensitive information due to events including but not limited to viruses, malicious attacks or system errors or omissions. This coverage could also include expense coverage for business interruption, breach management and/or mitigation services.[24]

Until issuance of the guidance, it was unclear whether cyber liability insurance was covered under the TRIA. However, the guidance confirms that stand-alone cyber insurance policies falling within the definition of cyber liability are included in the definition of "property and casualty insurance" under the TRIA and therefore are subject to the protections of the statute. In this regard, the guidance further states that effective April 1, 2017, insurers must provide disclosures and offers that comply with the TRIA and the regulations promulgated thereunder on any new or renewal policies reported as cyber liability insurance. Non-cyber liability policies that otherwise are covered by the TRIA and provide coverage for cyber risks have been, and will continue to be, subject to the TRIA.

The expansion of the TRIA to stand-alone cyber liability insurance policies provides security for policyholders and insurers alike and may have the benefit of accelerating market growth for stand-alone cyber liability insurance policies.

Return to Table of Contents

[23] U.S. Department of Treasury, *Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program*, December 2016, available here.

[24] *Id.*

Contacts in the Privacy and Cybersecurity 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

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@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

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@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

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

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

William Ridgway
Counsel / Chicago
312.407.0449
william.ridgway@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