Skadden

Privacy & Cybersecurity Update

1 The Impact of Brexit on the EU Data Protection Regime

2 Privacy Shield Nears Completion

2 German Data Protection Authority Fines Companies Who Followed Safe Harbor

3 Court Rules Cyber Insurance Policy Excludes Coverage for Significant Portion of Data Breach Costs

4 8th Circuit Upholds Coverage for Bank Under Financial Institution Bond for Cyber Hacker's Fraudulent Transfer

5 FTC and Fashion Industry Submit Comments on the Internet of Things

6 White House Releases Outline of Data Security and Privacy Principles for Electronic Patient Medical Information

7 California Court Allows Data Breach Suit Affecting 80 Million Consumers to Move Forward

8 Wisconsin Federal Court Dismisses Privacy Class Action for Lack of Standing Under *Spokeo*

9 FFIEC Issues Statement on Security of Interbank Messaging

The Impact of Brexit on the EU Data Protection Regime

Pundits are examining Brexit from many different angles. Below we discuss how it might impact the current state of EU data protection.

In some ways, Brexit could not have occurred at a less opportune time from an EU data protection perspective. Representatives from the U.S. and the EU are in the midst of finalizing the Privacy Shield to replace the Safe Harbor while seeking to address sharp criticism that has been leveled by EU regulators (see article below). In addition, the new EU data privacy law, the General Data Protection Regulation (GDPR), is in the final stages of being adopted, with a planned effective date of May 2018.[1] Until Brexit is completed, the U.K. is expected to adhere to the current EU data protection directive, accept the Privacy Shield and otherwise maintain the status quo (See Skadden's "Insights: Brexit" mailing). Moreover, because of a quirk in timing, the U.K. will even have to abide by the GDPR, as there will be a gap of several months between the effective date of the GDPR and the U.K.'s exit from the EU.

It remains to be seen what the U.K. will do when Brexit is completed. The U.K. will have a number of options, ranging from directly mirroring the GDPR and cross-border data transfer mechanisms such as the Privacy Shield (similar to Switzerland's mirror Safe Harbor mechanism these past few years), to creating an entirely new data protection construct that is substantially different from the EU approach. We anticipate that the U.K. likely will end up with a model closer to that of the EU model, but perhaps with a more "business friendly" approach that might appeal to the private sector. In this regard, the U.K. might follow the Canadian and Australian model of adopting privacy laws that are different from the EU, but still meet the EU standard of having "adequate" data protection laws so that personal information can flow easily and freely from the EU

[1] See our December 2015 *Privacy & Cybersecurity Update* for more on the GDPR.

to the U.K. We also expect that the U.K. will have finalized its approach before the GDPR goes into effect so that companies working toward GDPR compliance also can plan for the new U.K. regime. We will continue to closely monitor developments in this area.

Return to Table of Contents

Privacy Shield Nears Completion

U.S. and EU representatives have modified the Privacy Shield — which may go into effect in July — in an attempt to address criticism from various EU privacy regulators.

As we have reported in prior mailings,[2] the U.S. Department of Commerce and the European Commission have been working to finalize the Privacy Shield that will replace the Safe Harbor, thereby once again providing a "self-certification" mechanism by which companies can rely on to transfer personal information from the EU to the U.S. The Privacy Shield was necessitated by the October 2015 decision of the Court of Justice of the European Union to invalidate the Safe Harbor in the *Schrems* decision.

Since its release in February 2016, the Privacy Shield has come under sharp attacks from, among others, the European Data Protection Supervisor and the Article 29 Working Party, a European data protection advisory body whose membership comprises representatives from the data protection authority of each EU member state. United States and EU representatives reportedly have reached a compromise to address some of these critiques, including greater clarity involving "bulk data collection" by the U.S., the independent role of the ombudsman who is to oversee U.S. practices and a requirement that companies delete personal information when it is no longer required. Once these negotiations are concluded, the Privacy Shield will head to the Article 31 working group for approval. This group is comprised of representatives of the EU member states. While some have suggested the Privacy Shield will be completed in July, Article 31 members have stated that they will take as much time as they require to carefully review the Privacy Shield before approving it.

Return to Table of Contents

[2] For more information on the Privacy Shield, see our February 2016, March 2016 and May 2016 *Privacy & Cybersecurity Updates*, as well as our February 2, 2016 article.

German Data Protection Authority Fines Companies Who Followed Safe Harbor

The Hamburg, Germany, Data Protection Authority has fined six companies who had relied on the Safe Harbor for failing to adopt an alternative mechanism.

When the Court of Justice of the European Union invalidated the Safe Harbor in Schrems, many wondered what would happen to all the companies who suddenly found themselves out of compliance with the EU Data Protection Directive when they transmitted data from the EU to the U.S. Companies were relieved when the EU data protection authorities (DPAs) announced an informal six-month grace period while the Privacy Shield was finalized. When that six-month grace period expired, many assumed it would be informally extended with the Privacy Shield near completion. However, at least one DPA has taken a different view.

On June 6, 2016, the Hamburg, Germany, DPA issued a press release announcing that when the Safe Harbor was invalidated it had launched investigations into the data transfer activities of 35 companies. According to the DPA, most of these companies switched over to the model contracts, however, six did not and therefore were transferring data illegally to the U.S. According to the press release, three of these companies have been fined. The fines were reportedly minimal (approximately €10,000), with the low amount attributed to the fact that the companies had since switched to model contracts.

Practice Points

If the Privacy Shield does not, in fact, go into effect in the coming weeks (see above), then other DPAs may launch similar investigations and impose even larger fines. If this were to happen, companies may want to consider shifting over to the model contracts and not waiting for the finalization of the Privacy Shield.

Return to Table of Contents

Court Rules Cyber Insurance Policy Excludes Coverage for Significant Portion of Data Breach Costs

A federal judge determined that a policyholder is not entitled to coverage from its cyber insurer for over $1.9 million it paid out to a third-party credit card processing agent for assessments flowing from a large data breach, underscoring that all businesses procuring cyber insurance must carefully review policy language and be mindful of potential coverage gaps.

As companies across all industries are increasingly purchasing cyber insurance, a decision last month by the U.S. District Court for the District of Arizona serves as an important reminder that companies must exercise due care in selecting cyber coverage to ensure that it is appropriately tailored to adequately respond to their cybersecurity needs. In *P.F. Chang's China Bistro, Inc. v. Federal Ins. Co.*,[3] the court held that restaurant chain P.F. Chang's cyber insurance policy excluded coverage for roughly $1.9 million in credit card assessments incurred as a result of a large data breach, resulting in a coverage gap under the policy for a major portion of its data breach-related losses.

Merchants such as P.F. Chang's generally are not equipped to process credit card transactions directly with the banks issuing their customers' credit cards. As such, merchants typically contract with third-party acquiring banks to process their customers' credit card transactions with issuing banks. In the event of a data breach, credit card companies commonly assess fees on the acquiring bank, which the acquiring bank commonly passes off to the relevant merchant through indemnification provisions in their service agreements. This was the case in *P.F. Chang's*.

Prior to the data breach, P.F. Chang's had entered into a master service agreement (MSA) with an acquiring bank, Bank of America Merchant Services (BAMS), to facilitate the processing of credit card transactions with its customers. BAMS, in turn, entered into a separate agreement with MasterCard, which provided for the imposition of fees and assessments on BAMS in the event of a data breach. The MSA required P.F. Chang's to indemnify BAMS for these fees and assessments.

In June 2014, P.F. Chang's suffered a data breach when computer hackers obtained approximately 60,000 credit card numbers belonging to P.F. Chang's customers and posted this information on the internet. At the time of the breach, P.F. Chang's was insured by Federal (a Chubb company) under a cybersecurity policy.

P.F. Chang's promptly notified Federal of the incident and sought coverage for a variety of data breach-related costs, including the costs of conducting a forensic investigation into the data breach and defending litigation arising out of the breach. It also sought coverage for approximately $1.9 million it paid BAMS pursuant to the indemnification agreement in the MSA for a slew of fees assessed against it by MasterCard for fraudulent charges, notification and card replacement costs, and administrative fees arising from the breach. Federal provided over $1.7 million in coverage for the cost of the forensic investigation and the data breach-related litigation, but denied coverage for the $1.9 million in BAMS assessments.

In the ensuing insurance coverage litigation between P.F. Chang's and Federal, the court sided with Federal, holding that the policy did not cover the BAMS assessments. The court rebuffed P.F. Chang's argument that the assessments fell within the policy's coverage for losses arising out of claims for "Privacy Injury," which was defined to require that the compromised records belong to the actual claimant. The court reasoned that since the records compromised in the data breach belonged to P.F. Chang's customers and the card-issuing bank, not BAMS, BAMS itself did not sustain the requisite "Privacy Injury."

The court proceeded to conclude that coverage for the entirety of the BAMS assessments was unequivocally barred by two contractual liability exclusions and the policy's definition of "loss," which were drafted so as to exclude coverage for obligations the insured assumes by contract. The court found that "[i]n no less than three places in the MSA does [P.F.] Chang's agree to reimburse or compensate BAMS for 'fees,' 'fines,' 'penalties,' or 'assessments' imposed on BAMS by [MasterCard]." Accordingly, since P.F. Chang's liability for the BAMS assessments arose out of its undertaking in the MSA to indemnify BAMS for all such assessments, the policy's contractual liability exclusions and "loss" definition precluded coverage.

The court was unpersuaded by P.F. Chang's argument that the court should nevertheless find coverage for the BAMS assessments based on its reasonable expectations of coverage at the time it purchased the policy. The court reasoned that "[P.F.] Chang's and Federal are both sophisticated parties well versed in negotiating contractual claims, leading the Court to believe that they included in the Policy the terms they intended."

[3] No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016).

As the court's decision in *P.F. Chang's v. Federal* highlights, gaps in cyber insurance coverage can occur and can be costly. The cyber insurance market continues to evolve rapidly, and because policies are not standardized, coverage can vary widely. The risks covered by cyber policies, moreover, may not be fully understood by all businesses. Companies seeking to purchase or renew cyber coverage should therefore thoughtfully consider all available coverage options and carefully select a policy that is properly tailored to protect against the cyberrisks it faces.

Return to Table of Contents

8th Circuit Upholds Coverage for Bank Under Financial Institution Bond for Cyber Hacker's Fraudulent Transfer

In an encouraging decision for policyholders, the 8th Circuit has affirmed a district court's ruling that a bank is entitled to coverage under its financial institution bond for a fraudulent transfer that occurred after one of its employees inadvertently left the bank's computer network unsecured, allowing a cyber hacker to infiltrate the network.

A recent decision by the U.S. Court of Appeals for the 8th Circuit suggests that policyholders should not overlook traditional insurance and bond products in seeking coverage for claims arising out of cybersecurity breaches. In *State Bank of Bellingham v. BancInsure, Inc.*,[4] the 8th Circuit held that Minnesota-based State Bank of Bellingham was covered by its financial institution bond for a fraudulent wire transfer executed by a cyber hacker after a bank employee left the bank's computer network unsecured.

In October 2011, Bellingham's computer network became infected with malware, thereby enabling a cyber hacker to execute two fraudulent wire transfers of bank funds to foreign bank accounts. Bellingham performed wire transfers through a desktop computer connected to a specialized network device provided by the Federal Reserve. The network required bank employees to enter passwords, passphrases and physical security tokens to gain access to the network. The malware infection and resulting fraudulent transfers occurred when an employee left the physical security tokens in a desktop computer overnight after completing a legitimate wire transfer. Bellingham was unable to reverse one of the fraudulent transfers, resulting in a $485,000 loss.

Bellingham sought coverage for the incident from BancInsure pursuant to the terms of a financial institution bond it issued to Bellingham in 2010 that provided coverage for computer systems fraud. BancInsure denied coverage for the incident, citing a number of coverage exclusions, including one for employee-caused loss.

After the denial, Bellingham proceeded to file suit against BancInsure, alleging that its denial of coverage constituted a breach of contract. The district court concluded that Bellingham was covered under the bond for the fraudulent transfer, reasoning that the computer systems fraud was the "efficient and proximate cause" of the loss. In reaching this conclusion, the district court determined that the conduct of Bellingham's employees was not an independent cause of the loss because the fraudulent transfer was not a "foreseeable and natural consequence" of their conduct.

On appeal, the 8th Circuit affirmed, holding that "'the efficient and proximate cause' of the loss in this situation was the illegal transfer of the money and not the employees' violation of [Bellingham's] policies and procedures." Adopting the reasoning of the district court, the three-judge panel determined that an illegal wire transfer was not a foreseeable consequence of the bank employees' failure to follow proper computer security protocols and even if their negligence "'played an essential role' in the loss ... the ensuing loss of bank funds was not 'certain' or 'inevitable.'" The 8th Circuit's decision was based primarily on Minnesota's concurrent-causation doctrine, which provides that if an insured's loss resulted from a combination of covered and excluded risks, the insured is entitled to coverage so long as the excluded risk was not the overriding cause of the loss.

BancInsure had urged the panel to find that the concurrent-causation doctrine was inapplicable to financial institution bonds because they require the insured to initially demonstrate that its loss directly resulted from dishonest, criminal or malicious conduct, which, BancInsure contended, was a higher standard of proof than that provided for under the concurrent-causation doctrine. The panel was unpersuaded by this argument, predicting that since Minnesota treats financial institution bonds as insurance contracts, its courts would interpret such bonds in accordance with Minnesota's principles of insurance law, which include the concurrent-causation doctrine. The panel specifically rejected BancInsure's contention that financial institution bonds impose a higher standard of proof than the concurrent-causation doctrine, reasoning that "Bellingham still has to show that its loss was directly caused by the fraudulent transfer, and the application of the concurrent-causation doctrine did not interfere with that requirement."

[4] No. 14-3432, 2016 WL 2943161 (8th Cir. May 20, 2016).

The panel also rejected BancInsure's argument that certain exclusions in the bond were drafted so as to avoid application of the concurrent-causation doctrine. It noted that while parties may include "anti-concurrent causation" language in their agreement to prevent application of the concurrent-causation doctrine, in this case the bond exclusions' language referencing indirect causation was "not a sufficient invocation of the 'anti-concurrent causation' provision."

Although cyber insurance has become an important coverage line for businesses of all types to protect against cyber incidents, the 8th Circuit's decision in *State Bank of Bellingham v. BancInsure* demonstrates that traditional insurance policies and bonds also may provide coverage for such incidents, depending on the situation at hand and the language of the policy or bond. Therefore, in addressing a cyber incident, businesses are well-advised to meaningfully consider all potentially available coverages, including traditional insurance policies and bonds.

Return to Table of Contents

FTC and Fashion Industry Submit Comments on the Internet of Things

Recent statements by the FTC and the fashion industry regarding the internet of things highlight the balance that the industry and regulators are seeking to strike between privacy and the commercial value of internet-connected devices.

FTC Statement

On June 2, 2016, the staff of the Federal Trade Commission (FTC) issued a comment to the National Telecommunications & Information Administration (NTIA) on the internet of things (IoT), articulating benefits, risks and best practices for ensuring privacy and security.[5] As we previously have discussed[6] the IoT refers to physical devices connected wirelessly to the internet that collect, send and receive data. Examples of IoT objects include wearable health trackers that monitor heart rate and geolocation, built-in car sensors that track driving behaviors and remote-controlled thermostats that allow users to adjust the temperature of their homes. The IoT already has begun transforming the way individuals consume information, behave and interact, but there are significant risks presented by this new connectivity.

The FTC identified three major risks arising out of the massive collection and transmittal of data: risks to personal and network security, risks to privacy of sensitive information and risks to disadvantaged communities who may be underserved because they are under-connected.

In response to these concerns, the FTC articulated four best practices for businesses:

- **Security:** The FTC recommended that businesses take reasonable measures to ensure devices and networks are secure, including regularly updating product hardware and software. The FTC advises businesses to disclose to users when an IoT device is not secure for any reason; users will then be equipped to choose whether to transmit personal information.
- **Data Minimization:** Echoing the Privacy Protection Principles established by the Alliance of Automobile Manufacturers and the Association of Global Automakers in 2014,[7] the FTC called for IoT businesses to minimize the amount of data collected to only the information necessary to achieve the company's purposes. However, the FTC recognized that extreme restrictions may hinder potentially beneficial, future uses that currently are unknown.
- **Notice and Choice:** The FTC comment addressed two alternative approaches for limiting data collection. The first offers consumers a choice as to whether a specific type of data is collected; the second limits companies' collection based on "use" as defined by a regulatory entity. The FTC described the use-based restriction as inadequate because it fails to regulate when and what information is collected. Preferring the notice and choice approach, the FTC asked businesses to disclose to consumers when data is unexpectedly or inconsistently used and allow the customer to decide whether they want to allow it.
- **Big Data:** Lastly, the FTC called on businesses to analyze big data critically, with a focus on ensuring equitable distribution of resources. Because particular populations may not be aggregated into large data patterns, businesses analyzing IoT data should ensure meaningful patterns accurately reflect populations in need.

[5] The full text of the FTC's submission is available here.

[6] For earlier reports on the internet of things, see our January 2015, March 2015, May 2015 and September 2015 *Privacy & Cybersecurity Updates*.

[7] The Consumer Privacy Protection Principles are available here.

The FTC also noted the role that government should play in fostering and securing the IoT. In addition to meaningful enforcement efforts, the FTC called for "broad-based, technology-neutral, general privacy legislation." Other stakeholders, such as the Software & Information Industry Association,[8] fear that legislation specific to IoT concerns might risk over-burdening a still-developing technology space.

The fashion industry recently joined the list of industries commenting on the impact of the internet of things.[9] Although this industry may not seem like an interested party, as the world of IoT wearables expands, many designers realize they face growing security risks. The Fashion Innovation Alliance (FIA), in a June 2, 2016, letter to the NTIA, stated that it "values the privacy of the consumers using fashion tech products and services, and we recommend that any new policies governing IoT create an environment that supports and advances the ever-growing fashion tech industry without limiting innovation." To achieve this end, the FIA recommended the creation of a federally funded fashion tech innovation center that would bring the government's expertise in cybersecurity together with the fashion industry's entrepreneurial approach to design.

Practice Points

The FTC's proposal for general, technology-neutral privacy legislation is an attempt to resolve the tension between security, privacy and innovation. But legislation requiring companies to offer transparency and choice would not necessarily resolve the privacy and security risks posed by the IoT. The transparency and choice solution presumes a sophisticated consumer who understands the risks of allowing companies to collect and use data, and who takes time to weigh those risks against the benefits of using the IoT. Coupled with targeted enforcement by the FTC, however, general legislation may be sufficient in the current market. As IoT devices proliferate in the coming years, we expect the FTC to develop a more nuanced approach for protecting consumers' privacy and security interests with respect to the internet of things.

Return to Table of Contents

[8] The Software & Information Industry Association's response to the NTIA's request for comment is available here.

[9] The June 2, 2016, letter from the Fashion Innovation Alliance to the NTIA is available here.

White House Releases Outline of Data Security and Privacy Principles for Electronic Patient Medical Information

The executive branch recently released principles for how medical providers should implement security measures to protect their patients' personal data.

On May 25, 2016, the White House released a Data Security Policy Principles and Framework (PMI Data Security Framework)[10] for President Obama's Precision Medicine Initiative (PMI), a federal project analyzing how U.S. health care providers can provide more individualized and customized medical treatment to American patients in the future. In general, the PMI applies to federal agencies, public and private medical research institutes, and medical industry groups that are participating in large-scale investigative studies of common diseases like cancer, diabetes and heart disease.

The Data Security Framework, modeled after the National Institute of Standards and Technology Cybersecurity Framework (NIST Framework),[11] is a general statement of security and privacy principles for medical providers and consultants handling "PMI data," which is defined as patient-provided electronic data about their genomic, body chemical, dietary and environmental characteristics.[12]

The overarching theme of the PMI Data Security Framework is that medical providers and consultants handling PMI data should implement the "current best"[13] security measures to preserve the confidentiality and privacy of patient-provided PMI data. However, the PMI Data Security Framework explicitly states that PMI organizations are not required to implement the exact same PMI data security and privacy measures: "[T]here is no 'one size fits all' approach to managing data security…[o]rganizations can use the [Data Security Framework] to develop detailed implementation guidelines that address their specific data security needs."

[10] Available here. (hereinafter "DSF" in citations).

[11] A discussion of the NIST Framework is available here.

[12] See DSF, at p. 2.

[13] The PMI Data Security Framework does not define the term "current best," but notes that "security best practices are highly dependent on context" and that each PMI organization should undertake a "comprehensive risk assessment" to identify its own unique security requirements.

Nonetheless, the PMI Data Security Framework provides that at a minimum, a PMI organization, or an organization "conducting or participating in precision medicine activities," should: (1) implement de-identification encryption measures (which will de-couple a patient's name from his or her medical information); (2) protect PMI data with physical security controls, in addition to cybersecurity controls; (3) implement a system that would detect unauthorized breaches of PMI data, and audit uses of PMI data by authorized users; (4) create a response and recovery plan in the event of a PMI data breach; and (5) have an independent third party periodically conduct regular vulnerability assessments, in the form of network scans and penetration tests, to determine the effectiveness of the PMI organization's security plan.

The Data Security Framework also states that PMI organizations should "develop a policy for verifying the identity" of patients, but data security mechanisms should not be so onerous that patients are not able to easily access and re-transmit their own PMI data to other medical providers and professionals.

Next Steps

Although federal administrative agencies and research institutes with access to PMI data, such as the U.S. Department for Health and Human Services (HHS) and the National Institutes of Health (NIH), have "committed to integrate" the PMI Data Security Framework into activities involving PMI data, it is critical to note that the PMI Data Security Framework is neither a presidential executive order nor a federal agency regulation that carries the force of law and imposes data security requirements on private entities or businesses. Rather, the PMI Data Security Framework is simply a list of recommended best practices for private companies and health care providers handling PMI data to consider when drafting an entity-specific PMI data privacy program.

Furthermore, the White House stated in its online publication about the PMI Data Security Framework that none of the framework's data security and privacy principles are "intended to preclude the public posting of appropriate non-identifiable, non-individual level information, such as aggregate research data, research findings, and information about ongoing research studies."

Health care providers and consultants handling PMI data should be aware that the HHS's National Coordinator for Health Information Technology and NIST will, before December 2016, release a precision-medicine specific guide to the NIST Framework, which the White House says will provide further information on how PMI organizations can implement effective PMI data security and privacy systems.[14]

Return to Table of Contents

California Court Allows Data Breach Suit Affecting 80 Million Consumers to Move Forward

In *In re Anthem Data Breach Litigation*, Case No. 5:15-MD-02617 (N.D. Cal.), a California federal district court rejected health insurers' efforts to dispose of their insureds' claims for breach of contract, unfair business practices and unjust enrichment, holding that the plaintiffs had alleged sufficient facts to move forward with their claims.

On May 27, 2016, the United States District Court for the Northern District of California largely denied the motions of Anthem Inc. and other affiliated and non-affiliated health insurance companies to dismiss claims challenging the insurers' failure to maintain the safety of consumers' personal information. After previously dismissing many of the claims with leave to amend, the court held that the plaintiffs' second amended complaint alleged sufficient facts justifying portions of the suit to proceed.

Background and Claim

Anthem is one of the largest health insurance companies in the United States and is part of the Blue Cross Blue Shield health care network. In order to provide certain member services, Anthem, Blue Cross and other insurance companies collect personally identifiable information (such as Social Security numbers) and medical information (such as medical history) about their customers. Anthem maintained a database containing this information for approximately 80 million current and former customers of Anthem and affiliated and non-affiliated insurers.

[14] See framework here.

According to the plaintiffs, Anthem began having data security problems in 2009, when approximately 600,000 customers of WellPoint (Anthem's former trade name) were affected by a data breach. In 2013, the U.S. Department of Health and Human Services fined Anthem $1.7 million for various HIPAA violations relating to data security, and in 2014, the federal government warned Anthem and other health care companies of the possibility of cyberattacks, cautioning them to take appropriate preventative measures. In February 2015, Anthem announced that in January of that year, cyberattackers had breached the Anthem database and accessed the personal information of 80 million consumers.

Following Anthem's announcement, several putative class action lawsuits were filed, alleging that Anthem and more than 40 other affiliated and non-affiliated insurance companies failed to protect Anthem's data systems, failed to disclose to customers that Anthem did not have adequate security practices and failed to notify customers of the data breach in a timely manner. The plaintiffs alleged dozens of claims under state and federal law. The lawsuits were consolidated in multi-district litigation comprised of 127 cases.

As part of its case management process, the court ordered defendants to file limited motions to dismiss challenging 10 of the alleged claims. The court largely granted the motion with leave to amend. On March 11, 2016, the plaintiffs filed their second amended complaint, and defendants again moved to dismiss.

The Court's Decision

In a 90-page order, the court held that the plaintiffs had pleaded facts sufficient to proceed with certain breach of contract, unfair business practices and unjust enrichment claims. The court began with the plaintiffs' breach of contract claim under California law, which alleged that Anthem and its affiliates failed to protect consumers' information. After previously dismissing the claim for the plaintiffs' failure to identify any contract that was breached, the court sustained the amended claim. The court held that the plaintiffs had sufficiently alleged the existence of a contract, breach and damages by pleading that the insurers' promises to protect customers' privacy were incorporated by reference into their health insurance contracts and thus consumers could possibly recover damages for the lost benefit of their bargain, loss of value of their personal information and out-of-pocket costs incurred in dealing with the aftermath of the breach. The court reached a similar conclusion with respect to the plaintiffs' claim for breach of contract under New Jersey law.

The court also addressed the plaintiffs' claims for violation of the California unfair competition statute. The court held that the plaintiffs had standing to proceed with some of the claims because they alleged economic injury. With respect to the plaintiffs' claim that the insurers made a fraudulent misrepresentation or omission in violation of the unfair competition statute, the court held that the plaintiffs had alleged facts sufficient to proceed on the omission theory by pleading that they would not have enrolled in any of the policies had they known about Anthem's purportedly lax security practices. The court ruled that because the plaintiffs had sufficiently alleged fraudulent omission under California's statutory unfair competition law, they also had stated sufficient claims under New York's general business law.

The court's order differs significantly from the ruling on the defendants' prior motion to dismiss. In the prior ruling, the court held that none of the claims could proceed against the non-Anthem defendants. In reaching a different conclusion in the May 2016 order, the court noted that, unlike in the prior pleading, the plaintiffs' second amended complaint included enrollment data showing the number of residents in various states who carried policies with the non-Anthem defendants.

Key Takeaway

The *Anthem* decision highlights the potential exposure for companies in highly regulated and nationally monitored industries. Companies that maintain data for a significant number of customers should engage in early and frequent assessments and enhancements of their computer and data security practices and should carefully consider the impact of referencing separate privacy policies in any customer agreements.

Return to Table of Contents

Wisconsin Federal Court Dismisses Privacy Class Action for Lack of Standing Under *Spokeo*

In *Gubala v. Time Warner Cable, Inc.*, Case No. 2:15-cv-01078 (D. Wi.), a Wisconsin federal court dismissed a Time Warner Cable user's putative class action for lack of standing, holding that although the plaintiff alleged a violation of a statutory right, he failed to plead any concrete injury.

On June 17, 2016, a Wisconsin federal court dismissed a putative class action alleging that Time Warner Cable, Inc. illegally retained the private personal information of former customers. The decision highlights the impact of the U.S. Supreme Court's recent decision in *Spokeo, Inc. v. Robins*, No. 13-1339 (2016), which held that to establish Article III standing, a plaintiff must plead harm that is both particularized and concrete.

Background and Claim

On September 3, 2015, a former Time Warner Cable subscriber filed a putative class action against the company alleging that it illegally retained the personal information of former subscribers following termination of their subscriptions. The plaintiff alleged that he provided his personal information to Time Warner Cable when he subscribed in December 2004, and he terminated his service in September 2006. He alleged that he learned in December 2014 that Time Warner Cable was still retaining his information, which he alleged violated the Cable Communications Policy Act, requiring cable operators to destroy personally identifying information if it is no longer necessary.

In his original complaint, the plaintiff sought injunctive relief and damages. Time Warner Cable filed a motion to compel arbitration, asserting that the plaintiff's subscription agreement required claims for money damages to be resolved through binding arbitration. In response to Time Warner Cable's motion, the plaintiff filed an amended complaint, in which he deleted his request for money damages but continued to include extensive allegations about the economic value consumers place on the protection of their personally identifying information. Before any formal challenge was made to his amended complaint, the plaintiff was granted leave to file a second amended complaint seeking only injunctive relief. Time Warner Cable moved to dismiss that complaint, arguing that plaintiff had failed to properly plead entitlement to injunctive relief.

On May 16, 2016, the court heard oral argument on Time Warner Cable's motion to dismiss. The same day, the Supreme Court issued its decision in *Spokeo v. Robins*, holding that to have Article III standing, mere allegations of a statutory violation are insufficient; a plaintiff must plead she suffered injury that is both particularized and concrete. The Wisconsin court permitted the parties to submit briefing to address whether *Spokeo* had any impact on the plaintiff's case against Time Warner Cable.

The Court's Decision

Applying *Spokeo*, the Wisconsin court held that the plaintiff lacked standing to bring his case because he failed to plead he suffered any concrete harm as a result of Time Warner Cable's violation of the Cable Communications Policy Act. The court reasoned that "[a] statement that consumers highly value the privacy of their personally identifying information [] does not demonstrate that the plaintiff has suffered a concrete injury." The court remarked that unlike in *Spokeo*, the plaintiff did not allege that Time Warner Cable disclosed his information to a third party or made it publicly available. The court noted that even if the plaintiff had alleged such disclosure, he failed to plead he suffered any harm as a result of the hypothetical disclosure. The court rejected the plaintiff's argument that under a recent 7th Circuit decision, *Sterk v. Redbox*, the plaintiffs have Article III standing to sue for injunctive relief where a company wrongfully retains personal information. The Wisconsin court observed that *Sterk* held only that a federal court could issue an injunction if it had jurisdiction over the case.

The Wisconsin court further held that even if the plaintiff had standing to sue, dismissal would be appropriate because the plaintiff had an adequate remedy at law since damages are available for violation of the information destruction provision of the Cable Communications Policy Act. The court commented that the plaintiff simply dropped his request for damages because he wanted to avoid the arbitration provision in his subscriber agreement.

Key Takeaway

The Time Warner Cable decision highlights the continuing impact of *Spokeo*. Companies facing claims in federal court for statutory violations should scrutinize the complaints to determine if there is a basis for challenging standing due to lack of a particularized and concrete harm. This case also highlights the strategy, and illustrates the potential consequences of, including provisions in customer agreements requiring arbitration for claims seeking certain remedies.

Return to Table of Contents

FFIEC Issues Statement on Security of Interbank Messaging

The Federal Financial Institutions Examination Council recently issued best practices for financial institutions to follow when assessing cybersecurity risks in interbank messaging.

The Federal Financial Institutions Examination Council (FFIEC), which comprises, among other entities, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency, issued a statement in June reminding financial institutions of the need to actively manage and continuously assess the cybersecurity risks relating to interbank messaging and wholesale payment networks. Although not a regulation, the FFIEC statement, which

follows a series of cyberattacks, provides a good overview of the best practices companies should be taking. The FFIEC is particularly concerned with vulnerabilities in trusted client terminals running messaging and payment networks.

Proposed Risk Mitigation Steps

The FFIEC proposes a multi-layered approach to security controls that addresses the risk posed by compromised credentials. Specifically, financial institutions should take a number of steps, including:

- conducting ongoing information security risk assessments by taking into account new threat intelligence and identified risks;
- ensuring third-party service providers perform effective risk management and implement appropriate controls, including by testing their systems. Institutions also should ensure they are contractually obligated to provide security incident reports when issues arise that may affect the institution;
- ensuring protection and detection systems, such as intrusion detection systems and antivirus protection, are up to date, and firewall rules are configured properly and reviewed periodically (with the ability to detect abnormal activity);
- limiting the number of individuals who have system-wide privileges, and reviewing this list regularly to ensure it remains appropriate. More generally, having access-control procedures;
- implementing and testing controls around critical systems regularly, such as limiting the number of sign-on attempts. Report test results to senior management and, if appropriate, to the board of directors or a committee of the board of directors;
- implementing procedures for the destruction and disposal of media containing sensitive information based on risk relative to the sensitivity of the information and the type of media used to store the information;
- managing business continuity risk;
- conducting regular, mandatory information security awareness training, including how to identify and prevent successful phishing attempts, and ensuring the training reflects the functions performed by employees; and
- participating in industry information-sharing forums, such as FS-ISAC.

Return to Table of Contents

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

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

James R. 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 S. Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

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

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

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

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

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

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

Gregoire Bertrou
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@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

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