Skadden

Privacy & Cybersecurity Update

1 Sixth Circuit Reverses District Court's Dismissal for Lack of Article III Standing in Data Breach Suit and Revives Class Action Lawsuit

3 New York State Proposes Cybersecurity Regulation for Financial Institutions

3 FTC Comments on Compliance With NIST Cybersecurity Framework

4 FTC Chairwoman Highlights Need to Protect Against Ransomware Attacks

4 German DPA Issues Guidelines on Companies Using the EU-US Privacy Shield

5 CFTC Finalizes Safeguards Rule

Sixth Circuit Reverses District Court's Dismissal for Lack of Article III Standing in Data Breach Suit and Revives Class Action Lawsuit

In *Galaria v. Nationwide Mutual Ins. Co.*, the Sixth Circuit held that the plaintiffs in data breach class action lawsuits had Article III standing to bring claims for negligence and bailment. The holding, which reversed the district court's order dismissing the claims, follows recent Seventh Circuit precedent allowing injury-in-fact to be established by alleging a "substantial risk of harm."

On September 12, 2016, in an unpublished decision, a panel majority of the U.S. Court of Appeals for the Sixth Circuit held that plaintiffs alleging claims for negligence and bailment on behalf of a putative class affected by a data breach have Article III standing to assert the claims. The majority followed recent Seventh Circuit decisions allowing injury-in-fact to be satisfied by alleging a "substantial risk of harm" in data breach cases. This decision continues the recent trend of easing the allegations required to establish Article III standing in data breach cases.

Background and Claims

In October 2012, hackers breached the computer network of Nationwide Mutual Insurance Company (Nationwide) and stole the personal information of approximately 1.1 million individuals. The personal information included names, dates of birth, marital statuses, genders, occupations, employers, social security numbers and driver's license numbers.

Plaintiffs Anthony Hancox and Mohammed Galaria filed class action complaints in the U.S. District Court for the District of Kansas and the U.S. District Court for the Southern District of Ohio, respectively. Hancox's action was transferred to the Southern District of Ohio, which had designated the cases as related. The complaints allege that Nationwide willfully and negligently violated the Fair Credit Reporting Act (FCRA) by failing to adopt procedures to protect against wrongful dissemination of the plaintiffs' data, as well as claims for negligence, invasion of privacy by public disclosure of private

facts, and bailment arising out of Nationwide's failure to secure the plaintiffs' data against a breach.

The district court dismissed the complaints, concluding that (1) there was a lack of subject-matter jurisdiction over the FCRA claims because the plaintiffs did not have "statutory standing"; (2) the plaintiffs did not have Article III standing to bring the negligence and bailment claims because they did not allege a cognizable injury; and (3) the plaintiffs failed to state a claim for relief on their invasion-of-privacy claim. The plaintiffs appealed the dismissal of the FCRA, negligence and bailment claims, but did not appeal the dismissal of their invasion-of-privacy claim.

The Court's Decision

The Court of Appeals for the Sixth Circuit, in an unpublished decision, reversed the district court's dismissal of the FCRA, negligence and bailment claims. Writing for the majority, Judge Helene White held that, regarding the FCRA claims, the lack of statutory standing "does not implicate subject-matter jurisdiction." Instead, the lack of statutory standing should lead to dismissal for failure to state a claim. Accordingly, the majority reversed the district court's dismissal for lack of subject matter jurisdiction and remanded the matter to the district court to consider whether the complaints state a claim.

Regarding the negligence and bailment claims, the majority held that the plaintiffs' allegations were sufficient to plead Article III standing because the "Plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage." Essentially, the Sixth Circuit concluded that stolen data in the "hands of ill-intentioned criminals" sufficiently alleges a cognizable injury unlike the "speculative allegations of 'possible future injury' or 'objectively reasonable likelihood' of injury that the Supreme Court has explained are insufficient."

In reaching its decision, the majority applied the standard recently set forth by the Supreme Court in *Spokeo, Inc. v. Robins*, requiring plaintiffs to demonstrate that they "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of a defendant, and (3) that is likely to be redressed by a favorable judicial decision." The Sixth Circuit also followed recent decisions by the Seventh Circuit, which were decided before *Spokeo* and held that alleging a "substantial risk of harm" based on the theft of personal data was sufficient to establish standing. The majority specifically rejected the Third Circuit's contradictory holding for what is required to allege Article III injury at the pleading stage in data breach cases.

The majority also found that the complaints alleged causation sufficient to establish Article III standing by alleging that Nationwide "failed 'to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and other Class Members' [data] to protect against anticipated threats to the security or integrity of such information.'" Such allegations, the majority held, were in line with Seventh, Ninth and Eleventh Circuit decisions finding that Article III's traceability requirement was satisfied in similar data breach cases.

Dissenting, Judge Alice Batchelder argued that the majority erred in finding that the allegations in the complaints are sufficient to establish Article III standing. According to the dissent, the allegations in the complaints do not establish that the plaintiffs' injuries are traceable to Nationwide because the plaintiffs did not provide any "factual allegations regarding how the hackers were able to breach Nationwide's system [or] [] indicate what Nationwide might have done to prevent that breach but failed to do." That "*no one* prevented the data breach" did not give rise to a claim against Nationwide (or any other person) absent pleading specifically what Nationwide (or such other person) should have done and did not do that led to the data breach. Thus, the dissent would have held that no alleged facts plausibly demonstrate that Nationwide had any responsibility for the data breach, and that Article III standing was not properly alleged.

The dissent also argued for the dismissal of the FCRA claims based on the record because the plaintiffs did not state a claim for relief under the FCRA since Nationwide does not fall within the statute.

Key Takeaway

The Sixth Circuit's decision to follow the precedent of Seventh Circuit and find Article III standing where a plaintiff alleges that a data breach gave rise to a substantial risk of harm and where there are no specific allegations of what the defendant should have done differently continues the recent trend of courts easing the allegations required to establish Article III standing in data breach cases. The current circuit split concerning what allegations must be pleaded to establish Article III standing in data breach cases echoes the tension acknowledged by the Supreme Court in *Spokeo*, where the Court noted that a "concrete" injury is not necessarily synonymous with a "tangible" one. Until the Supreme Court weighs in on whether a substantial risk of harm in a data breach case is sufficiently concrete to confer standing, and what must be alleged for harm to be "fairly traceable" to the conduct of defendants, the determination of whether similarly pleaded cases will survive a motion to dismiss is likely to vary by circuit.

Return to Table of Contents

New York State Proposes Cybersecurity Regulation for Financial Institutions

New York state has proposed a new regulation — to go into effect January 1, 2017 — that would require banks, insurance companies and other financial services institutions regulated by the New York State Department of Financial Services (DFS) to establish and maintain a cybersecurity program. The proposal is the result, in part, of a DFS survey of approximately 200 regulated banking institutions and insurance companies regarding the industry's efforts to prevent cyberattacks.

For a complete analysis of the proposal please see the special edition of our *Privacy and Cybersecurity Update*, published earlier in September.

Return to Table of Contents

FTC Comments on Compliance With NIST Cybersecurity Framework

The FTC has commented on whether compliance with the NIST Framework constitutes sufficient cybersecurity protection for purposes of Section 5 of the FTC Act.

On August 31, 2016, the Federal Trade Commission (FTC) released an article designed to help companies determine whether compliance with the NIST Cybersecurity Framework ensures compliance with FTC cybersecurity requirements under Section 5 of the FTC Act.[1] Although much-awaited, the report fell short of providing concrete answers on which companies can rely.

Background on the NIST Cybersecurity Framework

In February 2014, the National Institute of Standards and Technology (NIST) released a set of industry standards and best practices to help critical infrastructure organizations manage cybersecurity risks. The framework does not require companies to engage in specific activities or comply with specific elements, but rather provides an open-ended framework for critical infrastructure companies to assess and establish cybersecurity policies and procedures in order to reduce the cyber risk those entities face.[2] The framework highlights the following five core functions that NIST considers part of a comprehensive view of cybersecurity risk:

- identifying which systems, assets and data require protection;
- protecting those systems, assets and data by implementing appropriate safeguards;
- detecting the occurrence of cybersecurity events
- responding to detected cybersecurity events; and
- recovering capabilities impaired through a cybersecurity event.

These categories are further subdivided into subcategories, along with cross-references to different existing industry and government standards that address the subcategories.[3]

FTC's Commentary on Compliance With the NIST Framework

Since its issuance, companies that are not critical infrastructure companies have wondered whether adhering to the NIST Framework effectively provided a "safe harbor" against FTC allegations that the company violated Section 5 of the FTC Act for failing to implement adequate cybersecurity safeguards.

This question arose because the FTC has not provided concrete rules or guidelines that entities can follow in order to ensure compliance with the FTC's cybersecurity requirements. Nonetheless, the U.S. District Court for the Third Circuit has upheld the FTC's authority to regulate cybersecurity generally, and, notably, rejected the argument that a company should receive notice of which specific cybersecurity practices are required to satisfy the standard under Section 5 of the FTC Act.[4]

The FTC's article states that, while the approach of the NIST Framework is generally consistent with the FTC's approach to cybersecurity, there is "really no such thing as 'complying with the Framework'"; instead, the article emphasizes that the FTC assesses reasonableness when considering a company's data security measures in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors. The FTC emphasizes that there is no "one-size-fits-all" approach to cybersecurity and that different types of organizations will require different

[1] 15 U.S. Code § 45.

[2] See "NIST Announces October Workshop and Releases Framework Update," *Skadden Privacy & Cybersecurity Update*, p. 1 (Aug. 2014).

[3] For a more detailed description of the NIST Framework, see "President Obama's Executive Order and Its Ramifications," *Skadden Privacy & Cybersecurity Update* (Jan. 16, 2014).

[4] *Federal Trade Commission v. Wyndham Worldwide Corporation*, 799 F.3d 236 (3rd Cir. 2015).

approaches to risk management.[5]

The article runs through each of the five core NIST Framework functions, emphasizing how each one corresponds with practices the FTC emphasizes in its enforcement of Section 5 of the FTC Act and highlighting cases the FTC has brought in which entities failed to take appropriate actions in accordance with such core functions. The article states that the framework can be used to serve as a model to conduct risk assessments and mitigations and to:

- establish or improve a data security program;
- review current data security practices; or
- communicate data security requirements with stakeholders.

The article also points to the FTC's publication, *Start with Security*, which summarizes issues from the FTC's data security cases and provides guidance to reduce cybersecurity risks.[6] In effect, although the FTC states that it is a good practice to follow the framework and its *Start with Security* guidelines, it still has not answered the question of what exactly is required in order to be compliant with FTC standards. Instead it emphasizes that there are no concrete steps that can be taken to ensure an entity will be in compliance.

Return to Table of Contents

FTC Chairwoman Highlights Need to Protect Against Ransomware Attacks

The FTC Chairwoman has cautioned that a failure to protect against ransomware attacks could constitute a violation of Section 5 of the FTC Act.

On September 7, 2016, FTC Chairwoman Edith Ramirez, speaking at the FTC's workshop on "ransomware" highlighted the prevalence of this relatively new tactic of cyberattacks. Ransomware is the term used to describe malware that infiltrates a computer system and then – typically through an encryption methodology – locks the victim's system until it pays a specified ransom. Ransomware hackers' "business model" is that victims will pay to prevent losing documents or data or having systems disabled. According to Chairwoman Ramirez, ransomware is the most profitable malware scam in history, and the practice is increasing at an alarming rate, with attackers typically using spam and spear phishing to target individuals or organizations.

Chairwoman Ramirez then put companies on notice that a failure to protect against ransomware attacks, specifically an unreasonable failure to patch vulnerabilities known to be exploited by ransomware, could be a violation of Section 5 of the FTC Act.

Although companies are generally implementing processes to block ransomware, the chairwoman's pronouncement further highlights the importance of taking this step.

Return to Table of Contents

German DPA Issues Guidelines on Companies Using the EU-US Privacy Shield

A German data protection authority has issued a statement and guidelines regarding use of the Privacy Shield.

On September 12, 2016, a German Data Protection Authority (die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI)) issued a statement and its own guidelines for companies transferring data to U.S. companies using the EU-U.S. Privacy Shield that the European Union and the United States have agreed upon. As part of that statement, the LDI highlighted concerns with the Privacy Shield, signalling that some data protection authorities may not be fully satisfied with this new regime.

Background

Current EU law forbids the transfer of personal data from EU countries to countries that do not have "adequate" data protection laws in place. Because the EU has concluded that U.S. privacy law does not meet the EU standard — and therefore companies would otherwise be unable to transfer personal data to the U.S. — the EU and the U.S. agreed on a "Safe Harbor" arrangement in July 2000 whereby companies could self-certify that they complied with certain privacy principles and then transfer personal data to the U.S. In October 2015, the EU Court invalidated the Safe Harbor framework based on the court's finding that it did not adequately protect the interests of EU data subjects.

On July 12, 2016, the European Commission formally adopted the EU-U.S. Privacy Shield, a privacy self-certification framework that will enable companies to transfer personal data from the European Union and the three European Economic Area member states (Norway, Liechtenstein and Iceland) to the U.S. The Department of Commerce began accepting self-certifica-

[5] Andrea Arias, "The NIST Cybersecurity Framework and the FTC," Federal Trade Commission (Aug. 31, 2016) can be found here.

[6] "Start with Security: A Guide for Business," Federal Trade Commission (June 2015), can be found here.

tions from companies on August 1, 2016.[7] Despite significant critiques of the Privacy Shield, the Article 29 Working Party (a data protection advisory body whose membership comprises representatives from the DPA of each EU member state) announced that DPAs would not challenge the Privacy Shield on their own initiative.

Statement and Guidelines by DPA

Despite the Article 29 Working Party announcement, the LDI has highlighted some concerns in relation to the Privacy Shield. In particular, the LDI warned German companies intending to transfer personal data of EU citizens to a U.S. company that they are obliged to verify in every single data transfer that the U.S. company:

- owns a valid certification (which has to be renewed annually), and the data to be transferred are covered by this certificate;
- can verify the compliance with its information obligations toward the relevant EU citizens; and
- has entered into contracts with third parties, to which the personal data shall be passed on, to assure the protection of this data.

Moreover, the LDI states that if a U.S. company processes personal data on behalf of a German company, the German company has to comply with the rules stipulated by Section 11 of the German Federal Data Protection Act.

Key Takeaways

Companies that intend to transfer personal data of German citizens to the U.S. should keep records regarding compliance with the abovementioned obligations before transferring such personal data. We also expect the LDI will not be the last DPA to weigh in on the Privacy Shield.

Return to Table of Contents

CFTC Finalizes Safeguards Rule

The CFTC has finalized its systems safeguard rules for U.S. commodities and derivatives firms, closely mirroring the proposal made in December 2015.

On September 8, 2016, the Commodity Futures Trading Commission (CFTC) finalized its systems safeguard rules for U.S. commodities and derivatives firms. The rules will be published in the Federal Register. These final rules were first proposed in December 2015[8], and the comment period for the proposed rules ended on February 22, 2016. The CFTC adopted the proposed rules, with a few modifications, based on the comments received. Most organizations will find they already comply with the new requirements, although perhaps not with the now-required frequency.

Derivatives clearing organizations and designated contract markets, swap execution facilities, and swap data repositories must comply with the requirements for vulnerability testing provisions and security incident response plan testing by March 20, 2017. They also must comply with the requirements for external penetration testing, internal penetration testing, controls testing and enterprise technology risk assessment by September 19, 2017. In addition, designated contract markets and swap data repositories must have testing of key controls by an independent contractor completed by September 19, 2019.

The final rules introduce five types of testing, specifying the frequency with which some tests must be administered and requiring that the board review the test results. Organizations that fail a test would have to establish a remediation plan to cure the applicable deficiency. The five testing types are:

- **Vulnerability Testing.** While most organizations already scan their systems for vulnerabilities, the new regulation would make this a formal requirement. Any automated vulnerability scanning must follow generally accepted best practices, and designated contract markets and swap data repositories will have to conduct such testing on a quarterly basis. Two tests must be conducted each year either by an independent contractor or by using employees of the organization who are not responsible for development or operation of the systems or capabilities being tested;
- **Penetration Testing.** Almost all guidance today lists penetration testing as a best practice to identify security risks. However, as with vulnerability testing, this will now be a formal regulation, with requirements to test for the risk of internal and external attacks;
- **Controls Testing.** In addition to testing for vulnerabilities, organizations will now be required to test, over a three-year rolling period, the key controls in their cybersecurity program, with large organizations required to conduct this testing using an independent contractor. Such testing "includes testing of all [of an organization's] system safeguards-related controls," such as which users have access to which data and systems;

[7] See Skadden's *Privacy and Cybersecurity Update* (July 2016) here.

[8] See Skadden's *Privacy & Cybersecurity Update* (December 2015) article for a discussion of the original proposal, here.

- **Security Incident Response Plan Testing.** Although implementing and testing security incident response plans (SIRPs) is a standard component of most organizations' cybersecurity programs, the regulation now imposes this as a formal requirement on CFTC-regulated entities; and
- **Enterprise Technology Risk Assessment.** Under the new regulations, organizations are required to conduct an annual assessment of the cybersecurity risks they face and the damage that would be caused by such incidents. Risk assessment should already be a standard component of organizations' cybersecurity planning, but the need to do this annually may require more frequent assessments, although subsequent assessments may be made by updating the previous assessment.

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