Skadden

Privacy & Cybersecurity Update

Ninth Circuit Finds in *Spokeo* Remand That Certain Statutory Violations Can Satisfy Article III's Standing Requirement

In a highly anticipated decision, the Ninth Circuit ruled that violations of the Fair Credit Reporting Act (FCRA) can give rise to a concrete injury that provides grounds for standing under Article III; however, the holding's fact-sensitive analysis may undermine its broad applicability.

On August 15, 2017, on remand from the U.S. Supreme Court, the Ninth Circuit ruled in *Robins v. Spokeo* (*Spokeo III*) that the violation of a consumer's statutory rights under the FCRA was sufficiently concrete and particularized to satisfy the standing requirement under Article III.[1] Following a review of the FCRA's text, purpose and legislative history, the Ninth Circuit found that the statutory harms alleged by the plaintiff were sufficiently concrete to meet Article III's injury-in-fact requirement.

Spokeo Procedural Background

In 2011, Thomas Robins sued Spokeo, a "people search engine" that, in response to user-generated requests, searches a wide array of sources to collect and report information about an individual, such as their address, phone number, marital status, age, occupation, hobbies and finances. In a putative class action, Robins claimed that a profile on Spokeo stated that he was married with children, in his 50s, relatively wealthy, and had a graduate degree and a job — all of which Robins asserted were inaccurate. Under the FCRA, Robins claimed that Spokeo willfully failed to comply with the requirement that consumer reporting agencies follow reasonable procedures to assure maximum possible accuracy of consumer reports. A district court in the Ninth Circuit heard the case and held that Robins had not pleaded an injury-in-fact necessary to establish Article III standing. On appeal, the Ninth Circuit reversed, stating that "the violation of a statutory right is usually a sufficient injury-in-fact to confer standing." The Ninth Circuit's decision (*Spokeo I*) further held that Robins' "personal interests in the handling of his credit

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

information [was] individualized rather than collective." On appeal, the case was granted a *writ of certiorari* by the Supreme Court, which issued a decision (*Spokeo II*) in May 2016.

The Supreme Court vacated and remanded the Ninth Circuit's decision in *Spokeo I*, holding that the circuit court used an "incomplete" analysis when it ruled that consumers can sue companies for statutory violations without alleging an actual injury. In a 6-2 decision, the Supreme Court held that when determining whether a plaintiff has standing to sue for statutory violations, courts must address both aspects of the injury-in-fact standing requirement — namely, whether the plaintiff suffered an injury that is both particular and concrete.

Businesses and consumer advocates alike hailed the *Spokeo II* decision as a win. Businesses facing "no-injury" class actions — those in which the alleged injury is simply a violation of a statute or regulation without an actual or imminent harm — embraced the decision, expecting it would make it easier for defendants to have such claims dismissed. Consumer advocates claimed the decision as a victory as well, commenting that the decision did not eliminate outright the ability to establish an Article III standing claim for intangible harms or a material risk of harm. Rather, the decision merely clarified the need to consider concreteness and particularization.

Ninth Circuit Reversal in *Spokeo III*

In reaching its decision on remand, the Ninth Circuit adopted a two-part test to determine whether the plaintiff's claim satisfied the "concrete" prong of Article III's injury requirement: (1) whether the statutory provisions at issue were established to protect the plaintiff's concrete interests as opposed to purely procedural rights; and (2) whether the specific procedural violations alleged actually harm, or present a material risk of harm, to such interests.

In applying the first part of the test, the court found that there is a "close relationship" between the harms contemplated by the FCRA and those traditionally protected by Congress, which has historically protected individuals against "untruthful disclosures." In reaching this conclusion, the court relied on two factors: (1) the ubiquity and importance of consumer reports in modern life and (2) the resemblance of FCRA's protections to "other reputational and privacy interests that have long been protected in the law." Moreover, the court opined that "it ma[de] sense" that Congress would not require "any additional showing of injury" beyond a violation of the FCRA. By drawing on the spirit and legislative history of the FCRA, the court concluded "that the [statute's] procedures at issue in this case were crafted to protect consumers' (like Robins) concrete interest in accurate credit reporting about themselves" and that his interests were "real, rather than purely legal creations" and "patent on their face."

In applying the second part of the test, the Ninth Circuit found that Robins alleged a "specific procedural violation" that actually harmed or presented a material risk of harm to his interests. While the Supreme Court in *Spokeo II* held that not all inaccurately reported information would create concrete harm under the FCRA, the Ninth Circuit found that in this case the nature of the alleged reporting inaccuracies were "substantially more likely to harm [Robins'] concrete interests than the Supreme Court's example of an incorrect zip code." Unlike an inaccurately reported zip code, the nature of the information on Robins was "the type that may be important to employers or others making use of a consumer report;" thus, his allegations "present[ed] a sincere risk of harm to the real-world interest that Congress chose to protect with the FCRA."

Key Takeaway

The ruling in *Spokeo III* provides guidance to litigants in identifying the types of procedural harms that satisfy standing requirements. However, the fact-sensitivity of the Ninth Circuit ruling and the reliance on the FCRA's legislative history suggest that the *Spokeo III* holding may be read narrowly.

Return to Table of Contents

DC Circuit's Reversal of Data Breach Case Deepens Circuit Split

In a decision that amplifies a circuit court split regarding standing in data breach lawsuits, the D.C. Circuit allowed a case to move forward against CareFirst BlueCross BlueShield (CareFirst) despite a lack of alleged actual identity theft by the plaintiffs.[2] This case joins a growing body of standing cases involving data breaches in the wake of the U.S. Supreme Court's holding in *Spokeo v. Robins*.

Background

The complaint arose out of a data breach experienced by CareFirst in June 2014, in which hackers accessed personal information of CareFirst policyholders, including names, birth dates, email addresses and health insurance policy subscriber

[2] A copy of the opinion is available here.

numbers. The district court concluded that the complaint did not allege that the hackers accessed the plaintiffs' Social Security and/or credit card numbers.[3] Applying *Spokeo, Inc. v. Robins*, which requires that the "injury in fact" alleged in the complaint must be "concrete, particularized, and … 'actual or imminent' rather than speculative," the district court found that the increased risk of identity theft due to the breach alleged in the complaint was not "actual or imminent" and dismissed the case.

The Appeal

On appeal, a unanimous three-judge D.C. Circuit panel reinstated the class action, finding that the plaintiffs' allegation of a substantial risk of identity theft stemming from the breach was sufficient to confer standing. The circuit court concluded that the district court erred in its interpretation of *Spokeo v. Robins* and noted that, according to guidance under *Clapper v. Amnesty International USA*, an injury may be sufficiently imminent when there is a "substantial risk" that it will happen.

The circuit court found that the complaint alleged substantial risks of both financial identity theft and medical identity theft. Unlike the district court, the circuit court concluded that the complaint did allege that the hackers gained access to Social Security numbers and credit card information in addition to names, birth dates, email addresses and policy subscriber numbers. The circuit court used "experience and common sense" to find a substantial risk of financial identity theft arising out of the hackers' access to this information. Importantly, the court did not solely rely on the exposure of Social Security and credit card numbers to reach its conclusion. It also found there to be substantial risk that an impostor could "impersonate the victim and obtain medical services in her name," even if the impostor had access only to the victim's non-financial information. These substantial risks of harm exist, according to the circuit court, "simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken."

Key Takeaway

With this decision, the D.C. Circuit joins a group of federal appeals courts, including the Third, Sixth, Ninth and Eleventh Circuits, that have smoothed the path to standing for data breach plaintiffs. The decision adds to the growing body of cases in which allegations of substantial risk of future injury are sufficient to confer standing. However, certain courts, including the Second Circuit and the Fourth Circuit, have refused to confer standing in arguably similar circumstances.

Return to Table of Contents

[3] See Skadden's August 2016 *Privacy and Cybersecurity Update* for a summary of the district court's decision.

Seventh Circuit Affirms Dismissal of FCRA Claims Due to Lack of Standing

The Seventh Circuit ruled that class action claims against two companies lacked standing based on the U.S. Supreme Court's decision in *Spokeo* that procedural violations without concrete harm are not sufficient to confer standing.

On August 1, 2017, the U.S. Court of Appeals for the Seventh Circuit affirmed the dismissal of class action suits against Time Warner Cable Inc. (TWC) and Great Lakes Higher Education Corp. (Great Lakes) alleging FCRA violations, holding that the plaintiff failed to plead sufficient injury to establish Article III standing under the U.S. Supreme Court's *Spokeo* decision.

Background

The plaintiff, Cory Groshek (Groshek), brought a class action suit against each of TWC and Great Lakes after the companies pulled his consumer credit reports as part of a job application process. Groshek alleged that the disclosure and authorization forms he had signed in connection with the application process violated the FCRA's stand-alone disclosure requirement because the forms contained extraneous information, including a release of liability. Under the FCRA, prospective employers may not obtain consumer reports for employment purposes unless (1) "a clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured … in a document that consists solely of the disclosure that a consumer report may be obtained for employment purposes" and (2) the consumer has authorized the procurement of the report by that person in writing.

The Court's Decision

The trial court dismissed the cases for lack of standing, relying on the *Spokeo* decision, which held that bare procedural violations divorced from concrete harm are not sufficient to confer standing. Groshek appealed the dismissals in a consolidated appeal to the Seventh Circuit, arguing that the trial court erred in finding that he lacked standing. A unanimous Seventh Circuit panel affirmed the lower court's decision, concluding that Groshek failed to demonstrate that he had suffered a concrete injury apart from the underlying statutory violation.

The court's analysis first considered Congress' intent in enacting the FCRA, stating that the stand-alone disclosure requirement was "clearly designed to decrease the risk of a job applicant unknowingly providing consent to the dissemination of his or her private information" and that the authorization requirement was

intended to further protect consumers from privacy violations by allowing jobseekers to withhold consent. The court noted that Groshek received a disclosure informing him that a background check would be conducted and that Groshek had simply alleged that the disclosure form contained extraneous information rather than arguing that this extraneous language confused him or "caused him not to understand the consent he was giving," or that he would not have given consent but for the extraneous information. Thus, the court found that Groshek had "alleged a statutory violation completely removed from any concrete harm or appreciable risk of harm."

The court rejected Groshek's claim that he had suffered informational injuries. Groshek had relied on two Supreme Court cases cited in *Spokeo* as instances where a violation of a procedural right was sufficient to constitute injury in fact. Both cases involved plaintiffs who sought to compel the government to disclose information that it was required to disclose pursuant to a statute. The court rejected Groshek's argument, finding that the injuries alleged in those cases were dissimilar because Groshek was not trying to compel TWC or Great Lakes to provide him with information. The court also found that Groshek had not suffered a privacy injury because he signed the disclosure form knowingly.

Finally, the court considered the Ninth Circuit's decision in *Syed v. M-I, LLC*, in which the Ninth Circuit held in a FCRA stand-alone disclosure case that the plaintiff had standing under *Spokeo*. The court distinguished this case because *Syed* had pled allegations from which the Ninth Circuit could infer harm — that the plaintiff was confused by the extraneous information provided and would not have signed the form had the disclosure been more clear. The court emphasized that unlike the plaintiff in *Syed*, Groshek presented "no factual allegations plausibly suggesting that he was confused by the disclosure form or the form's inclusion of a liability release, or that he would not have signed it had the disclosure complied" with the FCRA.

Key Takeaways

The Seventh Circuit's decision is another example of courts applying *Spokeo* to reject claims of statutory harm where plaintiffs fail to allege concrete injury. Unlike the *Spokeo III* and Carefirst cases discussed above, in this case the plaintiff did not allege any injury or risk of future injury. The ruling suggests that plaintiffs who allege only statutory violations are vulnerable to early dismissal and will find it difficult to establish standing in some jurisdictions.

Return to Table of Contents

UK to Pass Stricter Data Protection Law in Line With the GDPR

The United Kingdom has issued a statement of intent regarding a new data protection bill that is designed to make U.K. data protection laws consistent with the European Union's General Data Protection Regulation (GDPR), so the flow of data between the U.K. and the EU can continue uninterrupted post-Brexit.

On August 7, 2017, the U.K.'s Department for Digital, Culture Media and Sport issued a statement of intent regarding a new data protection bill (U.K. bill), which will establish greater safeguards for individuals than those currently under the U.K. Data Protection Act of 1998[4] and impose more obligations on companies collecting data. The U.K. bill aims to conform U.K. law to the European Union's GDPR in advance of Brexit. The GDPR will come into effect on May 25, 2018, when the U.K. will still be a member of the EU. When the U.K. leaves the EU, the U.K. bill will ensure that U.K. laws remain consistent with the GDPR. In its statement of intent, the U.K. government said the U.K. bill aims to promote the uninterrupted flow of data between the U.K. and EU. A date has not yet been set for debate of the U.K. bill in Parliament.

Expansions in Consumer Rights

Through various changes to U.K. law, the U.K. bill will provide consumers with greater control over how companies use personal information, while broadening the definition of "personal data" to include IP addresses, internet cookies and DNA. The rules surrounding "consent" to collect personal information also will be strengthened. For example, the use of default pre-checked "consent" boxes for collecting personal data will be prohibited, and consumers will be able to withdraw consent more easily.

The U.K. also will enact rules requiring organizations to inform individuals, at no charge, as to what personal data they are holding (so long as such requests from consumers are not "manifestly unfounded or excessive"). In addition, the U.K. bill will make it easier for consumers to move their data between service providers. Individuals also will have the right to require companies, including social media providers, to erase personal data held about them, bringing U.K. law in line with the EU's "right to be forgotten," which governs how search engines may index the personal data of EU citizens. The U.K. bill will provide protection against profiling based on the automated processing

[4] For the full statement of intent, see here.

of personal data, as in the case of online credit applications. Under the U.K. bill, individuals will be able to request that such processing be reviewed by a person rather than machine.

Stricter Enforcement

The forthcoming U.K. bill will increase the fines for data breaches and create two new criminal offenses. Currently, the maximum fine for a data breach is £500,000; under the new bill, larger fines of up to £17 million or 4 percent of a company's global turnover will be possible. In addition, the U.K. bill will criminalize intentionally or recklessly re-identifying individuals from anonymized or pseudonymized data. It also will criminalize altering records with the intent to prevent disclosure following an individual's data access request.

Permitted Derogations From the GDPR

The GDPR specifies that parents must consent to personal data processing on behalf of children and allows member states to set the threshold at any age from 13 to 16 years old at which a minor can consent to such processing without parental consent. Under the U.K. bill, children 13 years or older will be able to consent to personal data processing.

The GDPR only allows official authorities to process personal data on criminal convictions and offenses, but permits member states to allow other entities to process such data. Currently, the U.K. allows all organizations to process this type of data under certain circumstances, such as criminal record checks and the underwriting of driver's insurance. To preserve continuity with this aspect of the U.K.'s current data protection laws and to promote certain benefits, such as allowing organizations to protect themselves from potential criminal acts, the U.K. will continue to allow organizations other than those vested with official authority to process criminal convictions and offenses data.

Under the U.K. bill, journalists and scientific and historical research organizations will be exempt from specific aspects of the data protection laws if necessary to perform their functions in the public interest. For example, research organizations and archiving services will not be required to respond to individuals' data access requests when compliance would seriously impair or prevent them from fulfilling their purposes.

Key Takeaways

It was widely expected that the U.K. would strengthen its data protection laws to remain in step with the GDPR. By imposing greater requirements and penalties on companies that collect and process personal data of U.K. citizens, the U.K. bill should accomplish that goal. As a result, when the U.K. leaves the EU, companies should be able to freely transfer data between the U.K. and the EU. Companies should begin evaluating their U.K. data collection and processing practices and consider what steps they may need to take to conform to the new requirements. In addition, if a company's "main establishment" for data processing in the EU is currently in the U.K. such that the lead supervisory authority under the GDPR would be in the U.K., companies should be aware that after Brexit they may need to identify a different lead supervisory authority located in the EU, if there is another EU country in which management decisions are made regarding data processing activities. If there is no such location within the EU after Brexit, then the company's EU data processing activities may be subject to the jurisdiction of multiple member-state data protection authorities.

Return to Table of Contents

OCIE Releases Results of Cybersecurity Examination Initiative

The Office of Compliance Inspections and Examinations (OCIE) released findings from its recent cybersecurity initiative, which included areas of concern and also best practices recommendations for broker-dealers and investment advisers.

On August 7, 2017, the OCIE of the U.S. Securities and Exchange Commission (SEC) released a summary of its observations (the report) from cybersecurity examinations of 75 registered broker-dealers, investment advisers and investment companies that it conducted pursuant to the Cybersecurity Examination Initiative it announced on September 15, 2015 (the initiative).[5] The initiative's examinations focused on written policies and procedures regarding cybersecurity, with an increased focus on validating and testing that such policies and procedures were implemented and followed as compared to past reviews.

Background

On September 15, 2015, the SEC issued a risk alert release announcing OCIE's initiative,[6] under which it would undertake to examine registered broker-dealers and investment advisers' cybersecurity preparedness in light of recent breaches and

[5] The full text of the report is available here.

[6] OCIE, NEP Risk Alert, "OCIE's 2015 Cybersecurity Initiative" (September 15, 2015). A prior Skadden mailing regarding the initiative is available here.

continuing threats against financial services firms. The initiative was designed to build on OCIE's prior cybersecurity examinations conducted in 2014 and would review different firms than those from the prior initiative.

Key Findings

Overall, OCIE observed improvements in cybersecurity preparedness since its 2014 initiative, but also noted some areas for improvement and concern, which included:

- **Policies and procedures that were not sufficiently detailed.** Some policies and procedures were not reasonably tailored because they provided employees with only general guidance, identified limited examples of safeguards for employees to consider, were very narrowly scoped or omitted specific procedures for implementing policies.
- **Inconsistent enforcement of policies.** A number of firms did not enforce their own policies and procedures, or in some cases the written policies and procedures did not reflect the firms' actual practices. For example, written policies may require annual customer protection reviews, ongoing reviews of security protocols or completion of cybersecurity training, but, in practice, these reviews or procedures may be occurring less frequently than specified or not at all.
- **Inadequate system maintenance leading to violations of Regulation S-P.** The SEC's Regulation S-P requires investment advisers to adopt policies and procedures that address technical and physical safeguards to protect customer records and information. However, OCIE staff found Regulation S-P violations among firms that did not adequately conduct system maintenance, such as installing software patches to address security vulnerabilities or implementing additional operational safeguards.

OCIE Recommendations

OCIE staff also outlined a number of firms' practices and policies that should serve as best practices, including:

- **Maintaining an inventory of data, information and vendors.** Policies and procedures should include a complete inventory of data and information, with classifications of the risks, vulnerabilities, data, business consequences and information regarding each service provider and vendor.
- **Drafting detailed cybersecurity-related instructions.** In particular, details should be included for penetration tests, security monitoring and system auditing, access rights and reporting requirements.
- **Maintaining prescriptive schedules and processes for testing data integrity and vulnerabilities.** For example, patch management policies should include beta testing a patch with a small number of users and servers before deploying it firmwide.
- **Establishing and enforcing controls to access data and systems.** This includes implementing detailed "acceptable use" policies, requiring restrictions and controls for mobile devices, requiring third-party vendors to periodically log their activities on the firms' networks and immediately ceasing access of terminated employees.
- **Requiring mandatory employee training.** Information security training should be mandatory for all employees at time of hire and periodically thereafter, and firms should institute policies and procedures to ensure that employees complete the mandatory training.
- **Engaged senior management.** The policies and procedures should be vetted and approved by senior management.

Ransomware Attack Prevention

Additionally, on May 17, 2017, OCIE issued a cybersecurity risk alert (the ransomware alert) regarding the widespread ransomware attack known as WannaCry.[7] Similar to other ransomware attacks, WannaCry, infected computers with malicious software that encrypted computer users' files and demanded payment to restore access to the locked files. In the ransomware alert, broker-dealers and investment management companies were encouraged to (1) review the alert published by the United States Department of Homeland Security's Computer Emergency Readiness Team[8] and (2) evaluate whether applicable Microsoft patches for Windows XP, Windows 8 and Windows Server 2003 operating systems were properly and timely installed. The ransomware alert cautioned that smaller registrants may be at greater risk. It also pointed to observations from the initiative and outlined measures that firms should implement to mitigate the impact of ransomware attacks, including conducting: (1) periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities and potential business consequences, (2) penetration tests and vulnerability scans on systems that the firms considered to be critical and (3) regular system maintenance, including installing software patches to address security vulnerabilities.

[7] OCIE's "Cybersecurity: Ransomware Alert," is available here.

[8] The United States Department of Homeland Security's Computer Emergency Readiness Team alert is available here.

Conclusion

As noted in OCIE's "Examination Priorities for 2017,"[9] cybersecurity compliance and procedures remain a top priority. In light of OCIE's continued interest in promoting the Cybersecurity Examination Initiative, it would be prudent for broker-dealers, investment advisers and investment companies to review their cybersecurity policies and preparedness and develop a rapid response plan.

Return to Table of Contents

Delaware Expands Data Breach Notification Requirements

Companies that conduct business in Delaware will need to consider whether their current response plans surrounding data breaches meet the requirements of a new law that is set to take effect in 2018.

On August 17, 2017, the state of Delaware passed a law imposing stricter obligations on companies in the event of a data breach. The law, which goes into effect April 14, 2018, will require companies to inform Delaware residents affected by a data breach within 60 days following discovery of the breach and notify the state attorney general if a breach affects more than 500 residents.[10] Previously, companies were not required to notify the attorney general of data breaches. In addition, the law requires businesses that own, license or maintain personal information to implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use or disclosure of such information.

Definition of Personal Information

The revised law broadens the definition of "personal information" to include a Delaware resident's first and last name in combination with any one or more of the following: (1) Social Security number; (2) driver's license or state or federal identification number; (3) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a financial account; (4) passport number; (5) a username or email address in combination with a password or security question and answer that would permit access to an online account; (6) medical history, treatment or diagnosis by a health care professional or DNA profile; (7) health insurance identification number; (8) biometric data; and (9) individual taxpayer identification number.

Data Breach Notification

The law also changes the conditions that trigger the requirement to notify Delaware residents and the attorney general in the event of a data breach. Previously, companies were required to notify affected residents after investigating a data breach and concluding that a "misuse of information about a Delaware resident has occurred or is reasonably likely to occur." The revised law requires notice within 60 days following discovery of the breach unless a company investigation "reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached." We anticipate that companies likely will provide notification rather than take the risk that they have improperly determined no harm will result.

Credit Monitoring

If a data breach involves a Social Security number, companies must offer free credit monitoring services to the affected individuals for one year, unless the company has reasonably determined that the breach is unlikely to result in harm to the affected individuals. The Delaware State Chamber of Commerce criticized this aspect of the new law because of its potential to impose a disproportionate burden on small businesses that may be unable to meet the requirement's financial obligations.

Key Takeaways

Companies that conduct business in Delaware should consider whether their current practices and incident response plans meet the requirements of the new law and, if not, update such practices and plans prior to April 14, 2018.

Return to Table of Contents

Seventh Circuit Will Not Review Denial of Class Certification

The Seventh Circuit has declined to review a district court's decision to deny class certification in a data breach action against a health insurer for allegedly exposing insureds' personal identifiable information (PII).

On June 19, 2017, the U.S. Court of Appeals for the Seventh Circuit issued an order in *Dolmage v. Combined Insurance. Co. of America*[11] denying a Dillard's department store employee's petition to appeal a decision denying her motion for class

[9] OCIE's "Examination Priorities for 2017," are available here.

[10] For the full text of the law, see here.

[11] No. 17-8010, *petition denied* (Seventh Cir. June 19, 2017).

certification. The dispute against the company's health insurer stemmed from a data breach that exposed the PII of thousands of Dillard's employees.

The Data Breach

In 2011, plaintiff Anne Dolmage applied for an insurance plan underwritten by defendant Combined Insurance Company of America (Combined) through her employer Dillard's. Included with Dolmage's policy enrollment materials was a privacy pledge, which stated that Combined would not disclose her personal information except as permitted or required by law and outlined the safeguards in place to protect her personal data, including with respect to third parties. The Combined privacy pledge was part of the enrollment materials sent to all insured Dillard's employees.

Combined hired a third-party vendor, Enrolltek, to provide insurance support services to Dillard's employees. In connection with these services, Combined sent Enrolltek the PII of the insured Dillard's employees, including names, addresses, birth dates and social security numbers, which Enrolltek stored on its website. In July 2013, Combined learned that Enrolltek's website was not secure and the PII of Dolmage and thousands of other Dillard's employees had been publicly accessible on the internet for over a year. As a result of the data breach, Dolmage and numerous other Dillard's employees had their tax returns delayed, diverted or stolen by identity thieves.

The Putative Class Action

In May 2014, Dolmage commenced a putative class action against Combined in the U.S. District Court for the Northern District of Illinois, seeking class certification under F.R.C.P. 23(b)(3). Dolmage alleged, among other things, that Combined breached the privacy pledge included in the enrollment packages sent to all insured Dillard's employees by failing to ensure that Enrolltek securely maintained the PII of the insured Dillard's employees. According to Dolmage, the privacy pledge formed part of the Dillard's employees' insurance policies and therefore was legally enforceable. Combined, by contrast, took the position that the privacy pledge did not form part of the Dillard's employees' policies and therefore was not enforceable.

In November 2016, following the close of discovery, Dolmage moved for class certification pursuant to F.R.C.P. 23(b)(3) seeking to represent a class of over 4,000 Dillard's employees residing in nearly 30 different states whose PII was exposed as a result of the data breach.

The Class Certification Issue

In a May 2017 decision, the district court denied Dolmage's motion for class certification, concluding that the proposed class lacked commonality, typicality, predominance of common issues and superiority as required by F.R.C.P. 23(a) and 23(b)(3). The district court found that the enforceability of the privacy pledge, *i.e.*, whether it formed part of the putative class members' insurance policies, could not be determined on a class-wide basis. It reasoned that the proposed class covers residents in roughly 30 states and therefore the court would have to apply the laws of each of those states to resolve the issue, which generally renders class certification improper.

The district court also found that the issue of damages weighed against class certification because identity theft "is by its very nature a highly personalized crime," and therefore damages cannot be calculated on a class-wide basis. The court further noted that this was not a case where the court simply could determine liability on a class-wide basis and leave the issue of damages for a later stage because damages ordinarily are a key element of a breach of contract claim. Accordingly, the district court concluded that because "the individual issues overwhelm any common issues," class certification "was not the superior method of adjudicating the claims."

In her petition to the Seventh Circuit seeking leave to appeal the adverse class certification ruling, Dolmage argued that the district court erred in concluding that differences in state contract law precluded class certification. According to Dolmage, the district court failed to identify any likely or potential material differences in the relevant states' laws that would preclude class certification. "The application of multiple states' laws is no obstacle" to class certification, Dolmage argued, because "the enforceability issue can be resolved from the plain, substantially identical language in class members' contracts."

In opposing Dolmage's petition, Combined argued that the district court's decision should not be reviewed because it was based on a "straightforward and basic analysis and a routine application of longstanding class action law and principles." Combined also insisted that the district court correctly concluded that the individualized issues precluded certification, reasoning that calculating damages for thousands of class members "would be anything but simple, instead requiring thousands of mini-trials" and that the application of multiple states' laws would be required to resolve the privacy pledge enforceability issue.

In a one-page order, the Seventh Circuit sided with Combined, declining to hear Dolmage's appeal on the class certification issue.

Key Takeaway

While the Seventh Circuit's decision on class certification was a clear victory for Combined, Dolmage's lawsuit seeking to enforce the privacy pledge included along with her insurance policy continues to move forward on an individual basis. The district court's determination as to whether the privacy pledge forms a part of the policy and is therefore enforceable could have meaningful implications for future data breach disputes, as privacy pledges such as that at issue in *Dolmage v. Combined Insurance. Co. of America* have become commonplace among businesses of all types that collect personal consumer data.

Return to Table of Contents

Contacts in the Cybersecurity and Privacy Group

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

William Ridgway
Counsel / Chicago
312.407.0449
william.ridgway@skadden.com

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

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

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