Bloomberg Law

The United States
Law Week
Case Alert & Legal News™

Civil Procedure

Standing

In *Spokeo Inc. v. Robins*, the Supreme Court held that proving an injury-in-fact for Article III standing purposes requires showing that the injury actually exists and isn't speculative. Attorneys from Dentons US LLP look at the standard's current application in identity-theft cases. They also suggest ways to avoid liability in those cases, including proper notification after a data breach and the use of encryption.

Spokeo One Year Later: Courts Split Over Whether Identity Theft Risk Confers Standing After Data Breach

BY JOSHUA D. CURRY AND PETER Z. STOCKBURGER

Both before and after the U.S. Supreme Court's May 2016 decision in *Spokeo Inc. v. Robins*, in which the Court clarified the standard for alleging a sufficiently concrete ''injury-in-fact'' under Article III, the lower courts have wrestled with whether a plaintiff in a data-breach case who has alleged the threat of future identity theft has stated a sufficiently ''concrete'' injury to establish Article III standing to sue in federal court.

Although most courts have found the threat of future injury alone, without more, does not constitute a sufficiently concrete injury-in-fact for standing purposes, the circuit courts are split on what injury allegations are sufficient to satisfy this standard. The Sixth, Seventh, Ninth and D.C. Circuits have all recognized the threat of future injury in a data breach case can satisfy Article III's injury-in-fact requirement. The First, Second, Third and Fourth Circuits have disagreed.

We examine this circuit split by looking at the factors and facts used by the courts to determine whether allegations of threat of future identity theft are sufficient to establish the ''concrete'' injury required for standing purposes. We also provide some practical suggestions and identify trends in this evolving area of law.

Josh Curry is a Partner in Dentons' Atlanta Office, and is a member of the firm's Intellectual Property and Technology and Cybersecurity groups. Josh litigates intellectual property, technology, and cybersecurity and privacy cases. Peter Stockburger is a Senior Managing Associate in Dentons' San Diego office, and is a member of the firm's Global Employment and Cybersecurity groups. Peter focuses his practice on employment and cybersecurity litigation and counseling.

Spokeo, Clapper and Article III Standing

The Supreme Court has made clear that the ''irreducible constitutional minimum'' of Article III standing to sue in federal court consists of three elements: (1) injury-in-fact; (2) causation; and (3) redressability. *Lu-*

 ISSN 0148-8139

jan v. Defenders of Wildlife. To establish injury-in-fact, the plaintiff must show an invasion of a legally protected interest that is ''concrete and particularized'' and ''actual or imminent, not conjectural or hypothetical.''

In *Spokeo*, the Supreme Court reiterated and applied these standing requirements to a case arising under the Fair Credit Reporting Act (''FCRA''). There, the plaintiff alleged a FCRA violation after defendant Spokeo purportedly published incorrect information about the plaintiff on the company's people-search website, including information that purportedly would have hurt his employment prospects, dating prospects and/or reputation.

The district court dismissed the suit, citing a lack of standing for failure to plead an adequate injury-in-fact.

On appeal, the Ninth Circuit reversed, finding the alleged violation of the FCRA alone to be a sufficient injury-in-fact for standing purposes.

The Supreme Court reversed, and stated that a plaintiff cannot automatically satisfy Article III's injury-in-fact requirement whenever a statute grants a right and purports to authorize a suit to vindicate that right. Moreover, an injury-in-fact for standing purposes requires an injury that is ''concrete **and** particularized[.]'' (emphasis added).

Because the Ninth Circuit's analysis focused on ''particularity'' only and ignored the ''concreteness'' requirement, the Supreme Court remanded with instructions to consider both factors.

The Supreme Court in *Spokeo* explained that for an injury to be ''concrete,'' it must be ''*de facto*''—or in other words, the injury must ''actually exist'' and not be ''abstract.''

''Concrete'' is not synonymous with ''tangible.'' Although tangible injuries, like economic loss or physical harm, may be easier to recognize, an ''intangible'' injury can be sufficiently concrete to establish Article III standing if the intangible injury ''has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts[,]'' or if Congress has defined the particular injury as one that will '' 'give rise to a case or controversy where none existed before.' '' *Id*. (quoting *Lujan*, (Kennedy, J., concurring).)

Congress's role in identifying and elevating intangible harms, however, does not mean that alleging a statutory violation automatically satisfies the injury-in-fact requirement. Article III standing still requires a concrete injury.

Spokeo also cited the Court's 2013 decision in *Clapper v. Amnesty Int'l USA*, which held future intangible injury will be considered ''concrete'' for the purpose of Article III standing if it is ''certainly impending.''

In *Clapper*, the Court explained that ''certainly impending'' does not mean ''literally certain[.]'' Instead, standing may be found ''based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.''

The plaintiffs in *Clapper* were U.S.-based attorneys, human rights, labor and media organizations who alleged their work required them to communicate with foreign individuals who were likely targets of surveillance under the Foreign Intelligence Surveillance Act (''FISA''). The plaintiffs alleged an injury based on an ''objectively reasonable likelihood that their communications [would] be acquired'' under FISA ''at some point in the future.''

The Court rejected the plaintiffs' theory and found that the ''highly attenuated'' chain of possibilities underpinning their claims was ''too speculative'' to satisfy the requirement that the injury be ''certainly impending.''

Divergent Court Views on 'Concrete' Injury

Applying *Spokeo* and *Clapper*, the circuit courts appear to be split on the question of whether alleging the threat of future identify theft, alone, is sufficient to allege a concrete injury for standing purposes in data-breach and privacy cases.

Of the courts to address the issue, the Sixth, Seventh, Ninth, and D.C. Circuits have recognized that such allegations can establish an injury-in-fact. The First, Second, Third, and Fourth Circuits have come out in the opposite direction.

Threat of Future Identify Theft Sufficient

The Sixth, Seventh, Ninth, and D.C. Circuits have each found an allegation of a threat of future identity theft sufficient to state a concrete injury for standing under Article III where the plaintiff alleges his or her personal information was stolen for the purpose of obtaining and using that information to harm plaintiff.

In the Sixth Circuit's decision in *Galaria*, for example, the plaintiffs alleged ''hackers'' breached defendant's computer networks and directly ''stole the personal information'' of plaintiffs and 1.1 million others, creating an ''imminent, immediate and continuing increased risk'' of harm that the plaintiffs would be subject to future identity theft. The Sixth Circuit found these allegations to be sufficient to state a concrete injury under Article III because the ''hackers'' allegedly targeted plaintiffs' personal information directly.

Plaintiffs also alleged defendant had informed them of the breach in a letter that ''advised taking steps to prevent or mitigate misuse of the stolen data, including monitoring bank statements and credit reports for unusual activity[,]'' offered a ''year of free credit monitoring and identity-fraud protection of up to $1 million through a third-party vendor[,]'' and ''suggested that Plaintiffs set up a fraud alert and place a security freeze on their credit reports.''

According to the Sixth Circuit, because the plaintiffs alleged that the theft of their personal data placed them at a ''continuing, increased risk of'' fraud and identity theft beyond the speculative allegations of ''possible future injury'' that were found to be insufficient in *Clapper*, the court found there was no ''speculation'' because plaintiffs alleged their data had already been stolen and was ''now in the hands of ill-intentioned criminals.'' The court also noted that the defendant recognized the severity of the risk, ''given its offer to provide credit-monitoring and identity-theft protection for a full year.''

The Seventh Circuit reached a similar conclusion in *Remijas v. Neiman Marcus*, where the plaintiffs alleged ''hackers'' attacked Neiman Marcus and ''stole'' their credit card numbers. The plaintiffs also alleged that Neiman Marcus had learned fraudulent charges appeared on the credit cards of some its customers, discovered potential malware in its computer systems, publicly acknowledged the attack, and sent notification to customers who had incurred fraudulent charges on

   ISSN 0148-8139

their cards. The plaintiffs filed a putative class action complaint, alleging the ''hackers deliberately targeted Neiman Marcus in order to obtain their credit-card information[.]''

The court found the allegations to be sufficient under *Spokeo* and *Clapper* because they went ''far beyond'' those asserted in *Spokeo* by identifying an increased risk of future fraudulent charges and alleging the personal information was stolen directly by hackers for the purpose of targeting said information. According to the court, ''[w]hy else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.''

The Ninth Circuit in *Krottner v. Starbucks Corp.* reached a similar decision based on allegations that a laptop stolen from Starbucks contained the ''unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees.''

The plaintiffs alleged Starbucks sent a letter to affected employees, including plaintiffs, alerting them of the theft, and stating that Starbucks had ''no indication that the private information has been misused.'' Starbucks also stated in its letter that employees should monitor their financial accounts carefully for suspicious activity and take appropriate steps to protect themselves against potential identity theft. Starbucks offered affected employees credit monitoring services for one year.

Examining jurisprudence in other contexts wherein future injury was found sufficient to confer standing, such as in the context of environmental claims, the court found that the plaintiffs had alleged a ''credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data.''

If, however, the plaintiffs' allegations were ''more conjectural or hypothetical—for example, if no laptop had been stolen, and [plaintiffs] had sued based on the risk it would be stolen at some point in the future[,]'' the court would ''find the threat far less credible.''

District Courts in the Ninth Circuit have reached similar conclusions. *See, e.g.*, *In re Adobe Sys., Inc. Privacy Litig.* (finding allegations sufficient where hackers were alleged to have deliberately targeted Adobe's servers, spent several weeks collecting names, usernames, passwords, contact information and credit card numbers, and some of the stolen data had already surfaced on the internet); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.* (finding allegations sufficient where hackers allegedly stole personal information and the information was wrongfully disclosed as a result of the intrusion).

The D.C. Circuit in *Attias v. CareFirst*, characterizing standing at the pleadings stage as a ''low bar,'' determined standing was sufficient where plaintiffs alleged their ''credit card and social security numbers'' and ''health insurance subscriber ID numbers'' were stolen in a data breach.

The district court had dismissed plaintiffs' complaint for lack of Article III standing because it read the complaint as failing to allege theft of credit card or social security numbers. But the D.C. Circuit disagreed with this narrow reading of the complaint.

The D.C. Circuit noted plaintiffs' complaint defined the allegedly stolen information as including ''credit card and social security numbers,'' which the complaint alleged was information that identity thieves could use to open new financial accounts, incur charges in another person's name, and commit various other financial misdeeds. Thus, the appeals court found the complaint plausibly alleged the breach placed plaintiffs at a substantial risk of identity theft.

In addition, the D.C. Circuit found another independent basis for meeting Article III's injury-in-fact requirement: plaintiffs also alleged theft of their names, birthdates, email addresses, and ''health insurance subscriber ID numbers.'' The risk of ''medical identity theft'' in which a fraudster impersonates the victim and obtains medical services in her name, the court found, was an additional basis to find a substantial risk of identity fraud.

Citing the Seventh Circuit's decision in *Remijas*, the D.C. Circuit concluded the purpose of the hack was, sooner or later, to make fraudulent charges or assume those consumers' identities, and thus determined plaintiffs' had alleged a ''substantial risk of harm exists already, simply by virtue of the hack and then nature of the data that plaintiffs allege was taken.'' The court characterized this harm as ''much more substantial than the risk presented to the *Clapper* court,'' and sufficient to satisfy Article III's requirement of an injury in fact.

Threat of Future Identity Theft Insufficient

The First, Second, Third, and Fourth Circuits have come to different conclusions in similar cases.

In *Reilly v. Ceridian Corp.*, the Third Circuit found that the plaintiffs' alleged purported increased risk of identity theft was too hypothetical and speculative to establish a ''certainly impending'' injury-in-fact under Article III. There, the plaintiffs were employees of a law firm that had contracted with a third party for payroll services. That third-party suffered a security breach when ''unknown hackers'' infiltrated its system and ''potentially gained access to personal and financial information'' belonging to the plaintiffs.

The court noted it was ''not known whether the hacker read, copied, or understood the data.'' The payroll company sent letters to potential identity theft victims, informing them of the breach, and arranged to provide them with one year of free credit monitoring and identity theft protection.

Based on the facts, the plaintiffs alleged they suffered an ''increased risk of identity theft[.]''

The district court granted the defendants' motion to dismiss, and the Third Circuit affirmed.

According to the Third Circuit, the plaintiffs' allegations were too ''hypothetical'' because they relied on ''speculation that the hacker: (1) read, copied, and understood their personal information; (2) intended to commit future criminal acts by misusing the information; and (3) was able to use such information to the detriment of [plaintiffs] by making unauthorized transactions in [their] names.''

The court stated that unless and until these ''conjectures come true,'' plaintiffs have ''not suffered any injury; there has been no misuse of the information, and thus, no harm.''

The Third Circuit held unless a plaintiff's 'conjectures come true,' they haven't 'suffered any injury; there has been no misuse of the information, and thus, no harm.'

Likewise, in *Katz v. Pershing*, the First Circuit found that a brokerage account-holder's increased risk of unauthorized access and identity theft was insufficient to establish an ''actual or impending injury'' after the defendant failed to properly maintain an electronic platform containing her account information.

The plaintiff alleged that ''there is an increased risk that someone might access her data and that this unauthorized access (if it occurs) will increase the risk of identity theft and other inauspicious consequences.''

The court found that ''the risk of harm that she envisions is unanchored to any actual incident of data breach.'' Therefore, the court found this ''omission [to be] fatal; because she does not identify any incident in which her data has ever been accessed by an unauthorized person, she cannot satisfy Article III's requirement of actual or impending injury.''

In the Fourth Circuit's decision in *Beck v. McDonald*, plaintiffs alleged that an unencrypted laptop computer and four boxes of pathology reports, each containing private medical information, were stolen from a Veteran's Affairs center.

Relying on *Clapper*, the Fourth Circuit found that the plaintiffs failed to state a ''certainly impending'' injury because even after extensive discovery they uncovered no evidence that the information contained on the stolen laptop or in the four missing boxes of medical records had been ''accessed or misused'' or that the materials had been stolen with the intent to steal ''private information.''

The Fourth Circuit analyzed the circuit split discussed above, and distinguished the decisions in *Galaria* and *Remijas* on the basis that each had ''common allegations that sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent,'' including the allegation that the ''data thief intentionally targeted the personal information compromised in the data breaches.'' In contrast in *Katz* and *Reilly*, the Fourth Circuit noted that no such allegations were present. The Fourth Circuit also rejected the Sixth Circuit's inference of a substantial risk of harm of future identity theft based on ''an organization's offer to provide free credit monitoring services to affected individuals[,]'' and recognized that as breaches fade further into the past, the plaintiffs' threatened injuries ''become more and more speculative.''

Finally, and most recently, the Second Circuit, in *Whalen v. Michaels Stores, Inc.*, affirmed a District Court's dismissal of claims for breach of implied contract for lack of standing because the plaintiff failed to allege a cognizable injury ''from the exposure of her credit card information following a data breach at one of Michaels' stores.''

The plaintiff in *Whalen* made purchases via credit card at a Michaels store on Dec. 31, 2013. On Jan. 14 and 15, unauthorized attempts were made to charge over $1,500 to her card, but no fraudulent charges were actually incurred, and she canceled her card on Jan. 15, 2014.

On Jan. 25, 2014, Michaels issued a press release saying there had been a possible data breach of its system involving theft of customer credit card and debit card data. The company offered potential victims of the attack 12 months of identity protection and credit monitoring services.

The District Court held the allegations did not suffice to establish Article III standing because the plaintiff did not allege she incurred ''any actual charges on her credit card, nor, with any specificity, that she had spent time or money monitoring her credit.''

The Second Circuit agreed, holding that the plaintiff did not allege a ''particularized and concrete injury'' because she ''never was either asked to pay, nor did pay, any fraudulent charge[,]'' and because she did not allege ''how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information - such as her birth date or Social Security number'' was alleged to have been stolen. The court also noted that the plaintiff plead no ''specifics about any time or effort that she herself has spent monitoring her credit.''

District Courts following these standards have likewise rejected standing where insufficient facts were pled to show the bad actor specifically targeted the plaintiffs' personal information. *See, e.g., Polanco v. Omnicell, Inc.* (unclear from allegations whether the plaintiffs' information was taken); *Storm v. Paytime, Inc.* (plaintiff did not allege information was misused or that misuse was impending).

Takeaways

As the courts continue to wrestle with these difficult questions, the following key takeaways and trends are notable:

■ **Be Careful How the Breach Is Described**: Entities should take care in how a breach is described when notifying affected individuals. If the notification describes the suspected bad actor and motivations with particularity, for example, affected individuals may use that language to allege a concrete injury. Entities should be cognizant of the myriad state laws that require detailed notification, and coordinate with litigation counsel to ensure compliance with state law does not unnecessarily expose the entity to future liability in data-breach litigation.

■ **No Good Deed Goes Unpunished**: Offering mitigation services after a breach may come back against the entity in data-breach litigation. In *Galaria*, for example, the Sixth Circuit used that exact behavior to bolster its finding that the plaintiff had pled a sufficient concrete injury. Although the Fourth Circuit rejected this approach in *Beck*, entities should nonetheless be aware that offering services outside of those required by state law may expose the entity to future liability.

■ **Use Encryption**: If data is encrypted, there may be a stronger defense available to challenge standing. In

  LW ISSN 0148-8139

Krottner, for example, the Ninth Circuit found that the plaintiffs had alleged a credible threat of real and immediate harm, in part, because the laptop stolen contained unencrypted personal data. Likewise, in *Adobe*, a district court found that the bad actors were able to decrypt the personal information of the plaintiffs and expose them to future injury, because the encryption software used was deemed insufficient under industry standards. In *Beck*, however, the personal information on the stolen laptop was unencrypted, but the court did not discuss this issue when it found the allegations to be insufficient to establish standing. These cases illustrate the importance of quality and industry-tested encryption when storing personal information, which is often required under state law.

■ **Defenses After the Pleadings Stage:** Even if a motion to dismiss to challenge standing is not successful, a similar motion at the summary judgment stage may be successful. The timing of the breach, for example, may provide an argument that the threat of future injury has been mitigated (e.g., because no harm has been demonstrated during discovery in the case). The Seventh Circuit in *Remijas* and the Fourth Circuit in *Beck* both recognized the potential viability of this defense. The individualized nature of each plaintiff's threat of future injury may also serve as a defense against class certification under Federal Rule of Civil Procedure 23.

■ **Don't Forget Causation and Redressability**: Although the focus of this article is on the first element of standing, that of injury-in-fact, the two other elements of standing, causation and redressability, are also important to consider. The Sixth Circuit in *Galaria*, for example, examined all three. The Ninth Circuit in *Krottner* only addressed injury-in-fact. And the dissenting opinion in *Beck* noted that the Fourth Circuit should have affirmed the order dismissing the underlying complaint on the issue of causation and not injury-in-fact. All three elements should be examined carefully in data-breach litigation to determine if there is standing under Article III.

Conclusion

Data breaches are not slowing down. As technology develops, the capability to attribute malicious cyber activity becomes more certain, and challenges to standing in data-breach litigation continue to evolve, businesses must stay alert in this area of the law and monitor court developments in order to prepare for and to mitigate against future harm and liability.