Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 34, ISSUE 23 / APRIL 21, 2017

EXPERT ANALYSIS

# Data Security Breach Litigation Post-*Spokeo*

**By Elizabeth E. McGinn, Esq., James T. Shreve, Esq. and Daniel Paluch, Esq.**
***Buckley Sandler LLP***

California enacted the nation's first data security breach notification law 15 years ago.[1] Following a few high-profile incidents in 2005, other states rapidly began enacting breach-notice requirements based largely on the California model.[2]

This proliferation of laws — and the constant news of security incidents — led many to predict a significant increase in data security breach litigation.

While nearly every jurisdiction in the U.S. has adopted similar breach notification laws, there has not been a tidal wave of successful private litigation relating to data security breaches.[3] Why?

To this point the reason is, in a word, standing. Standing is a prerequisite to bringing a lawsuit in federal court. It derives from Article III of the U.S. Constitution.

The Supreme Court noted in *Clapper v. Amnesty International USA* that Article III standing requires that "an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'"[4]

Plaintiffs in security breach litigation have had difficulty surviving defense arguments that they lack standing to sue.

Although data security breach notification laws are meant to require or encourage the protection of consumers' data, many do not explicitly give consumers a private right of action. This means, by themselves, violations of these laws frequently are insufficient to give consumers standing to sue because some form of legally recognized injury is necessary to establish Article III standing to pursue a claim in federal court.

The fact that a data security breach has occurred, or that a company has failed to notify a consumer of that breach, does not necessarily mean that a consumer has been injured. Thus, in data security breach cases, courts have focused on the purported injuries plaintiffs claim to have suffered and what kinds of breach-related injuries can confer standing.

Based on the holding in *Clapper* and previous cases, many data breach cases were dismissed at the pleadings stage. However, some plaintiffs were able to survive dismissal motions and thus increase their chances of a more favorable settlement.

For example, in *Remijas v. Neiman Marcus Group LLC*,[5] the 7th U.S. Circuit Court of Appeals revived a potential data breach class action against department store chain Neiman Marcus.

The trial court had dismissed the case on the basis that the plaintiffs' alleged future harm was not sufficiently concrete.

The 7th Circuit reasoned that it was plausible to infer that hackers stole plaintiffs' credit card numbers from Neiman Marcus so that they could use them in the future.

*While nearly every jurisdiction in the U.S. has adopted breach notification laws, there has not been a tidal wave of successful private litigation relating to data security breaches.*

Because of this elevated risk of future fraudulent charges, the 7th Circuit concluded that the plaintiffs had alleged an "objectively reasonable likelihood" that future harm would occur and had standing to pursue their claims on that basis.

The 7th Circuit remanded the case to the trial court for further proceedings.

Last year, there was some indication that the Supreme Court's decision in *Spokeo Inc. v. Robins*[6] would clarify questions of standing relevant to data security breach cases.

Spokeo is a website that aggregates information about people. It allegedly disseminated incorrect information about the plaintiff, a Virginia man named Thomas Robins.

Robins filed a lawsuit in federal court, claiming that Spokeo's dissemination of the inaccurate information about him violated the Fair Credit Reporting Act. That law requires companies like Spokeo to "follow reasonable procedures to ensure maximum possible accuracy" of the information that it makes available for use in credit reports.

The trial court dismissed the plaintiff's complaint for lack of standing, but the 9th Circuit reversed.

Because the plaintiff had a personal interest in the handling of his credit information, the 9th Circuit held that he had suffered a particularized harm that gave him standing to sue.

In reviewing the 9th Circuit's decision, the Supreme Court noted that while particularization is necessary, it is not sufficient. Rather, the high court stated, an injury-in-fact must also be concrete, an issue the 9th Circuit failed to sufficiently consider.

Buttressing its earlier decisions on Article III standing, the high court reasoned that a risk of harm can satisfy the requirement of concreteness. However, because the plaintiff had not alleged more than a procedural violation of the FCRA — he had not alleged any actual, concrete harm based on the allegedly inaccurate information Spokeo published online — he could not meet the requirements of Article III standing.

Many observers believed *Spokeo* would cause fewer data security breach cases to advance in the courts.

However, despite the Supreme Court's focus on concrete harm, and data security breach plaintiffs' previous difficulties alleging such harm, the initial results post-*Spokeo* have been mixed.

Some courts have dismissed data breach cases for lack of standing based on a failure to allege concrete harm.[7]

However, other courts have been more hesitant to use *Spokeo* to dismiss breach-related claims and have permitted them to continue even without clear allegations of damages beyond statutory violations.

In the Horizon Healthcare Services Inc. data breach, two laptops containing the unencrypted sensitive personal information of more than 839,000 Horizon plan members were stolen from the company's headquarters.[8]

As a result of the theft, the plaintiffs had their Social Security numbers compromised. One of them alleged that the stolen data was used to file a fraudulent tax return in his name.

To recover for these damages, the plaintiffs filed a class action complaint alleging violations of the FCRA and various state laws. The FCRA section they relied on prohibits unlawful disclosure of legally protected information and allows recovery of statutory damages for those violations.

The trial court dismissed the complaint for lack of standing. It concluded that the plaintiffs had not alleged a sufficient injury-in-fact because they had not suffered a cognizable injury caused by the data breach.

The court rejected the plaintiffs' argument that Horizon's alleged violation of the FCRA alone conferred standing, explaining that standing requires "some form of additional, 'specific harm' beyond 'mere violations of statutory and common law rights.'"

On appeal, the 3rd Circuit arrived at the opposite conclusion. It ruled that the plaintiffs did not have to allege that their information had been misused but instead could rely on purported violations of the FCRA to establish standing.

While the court in *Spokeo* held that consumers must allege a tangible or intangible concrete injury and cannot rely solely on a mere procedural violation divorced from concrete harm to establish Article III standing, the high court also acknowledged that "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact."

The 3rd Circuit panel relied on this holding in resurrecting the Horizon policyholders' FCRA claims, saying they had established a sufficiently concrete injury by asserting that the insurer ran afoul of the FCRA by failing to protect their unencrypted sensitive information.

"In light of the congressional decision to create a remedy for the unauthorized transfer of personal information, a violation of FCRA gives rise to an injury sufficient for Article III standing purposes," Judge Kent A. Jordan wrote. "Even without evidence that the plaintiffs' information was in fact used improperly, the alleged disclosure of their personal information created a de facto injury."[9]

*Plaintiffs in security breach litigation have had difficulty surviving defense arguments that they lack standing to sue.*

The 6th U.S. Circuit Court of Appeals also found that a violation of the FCRA that created a substantial risk of harm was sufficient to establish standing under *Spokeo*.

In *Galaria v. Nationwide Mutual Insurance Co.*,[10] two customers of the insurance company brought a class action against the company after hackers breached its computer network and stole their personal information.

The plaintiffs' initial complaint did not allege any misuse of the stolen data; rather, it alleged a future risk of harm due to identify theft.

The trial court dismissed the plaintiffs' claims, holding that "the increased risk that plaintiffs will be victims of identity theft, identity fraud, medical fraud or phishing at some indeterminate point in the future" does not necessarily confer standing.

While the 6th Circuit noted that it was not certain that the plaintiffs' data would be misused, it concluded that there was a sufficiently substantial risk of harm that plaintiffs would, at the very least, incur costs related to mitigating the identity theft they had suffered.

Concluding that these costs were sufficiently concrete to satisfy the injury requirement of Article III standing, the court reversed the dismissal of plaintiffs' claims.

The 3rd Circuit's ruling in the Horizon Healthcare case and the 6th Circuit's ruling in *Galaria* show that some federal appellate courts may find standing for a de facto injury that results from a violation of the FCRA itself even without additional specific harm.

The 3rd Circuit's reasoning is a departure from prior cases in which it and other federal and state courts have said that fear of future identity theft alone does not establish Article III standing.

As these opinions show, courts continue to wrestle with how to apply *Spokeo*. The circuit courts are still split, signaling that the issue could return to the Supreme Court for further clarification or lead legislators to address the issue statutorily.

## NOTES

[1] S.B. 1386, 2001-2002 Reg. Sess. (Cal. 2002).

[2] Forty-seven states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands have enacted breach notification statutes. New Mexico is in the process of enacting a similar requirement.

[3] *See, e.g.*, Sasha Romanosky et al., *Empirical Analysis of Data Breach Litig.*, 11 J. Empirical Legal Stud. 74 (2014).

[4] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (citing *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139 (2010)).

[5] 794 F.3d 688 (7th Cir. 2015).

[6] 136 S. Ct. 1540 (2016).

[7] *See, e.g., Beck v. McDonald,* 848 F.3d 262 (4th Cir. 2017) (plaintiffs lacked standing because of a failure to plead that harm from identity theft was "certainly impending" or that there was a "substantial risk" that the harm would occur); *see also Dugas v. Starwood Hotels & Resorts Worldwide Inc.,* No. 16-cv-14, 2016 WL 6523428, at *6 (S.D. Cal. Nov. 3, 2016) (court dismissed a claim for theft of personal identifying information, holding that allegations of such a theft, without more, do not demonstrate "a harm that qualifies as an injury in fact for standing purposes"); *see also Attias v. CareFirst Inc.,* 199 F. Supp. 3d 193, 202 (D.D.C. 2016) (dismissed claims brought against an insurer for its alleged failure to safeguard its customers' personal information by holding that statutory violations alone do not render an injury concrete if a plaintiff would not otherwise have Article III standing.).

[8] *In re Horizon Healthcare Servs. Inc. Data Breach Litig.,* 846 F.3d 625 (3d Cir. 2017).

[9] The panel noted that the 3rd Circuit's pronouncements on Article III standing in recent years "have not been entirely consistent," pointing out that in some cases, including *Doe v. National Board of Medical Examiners,* 199 F.3d 146 (3d Cir. 1999), and *Fair Housing Council of Suburban Philadelphia v. Main Line Times,* 141 F.3d 439 (3d Cir. 1998), the circuit has appeared to reject the idea that the violation of a statute can on its own support Article III standing, while in others it has accepted the argument that in some circumstances the breach of a statute is enough to cause a cognizable injury even without tangible harm.

[10] 663 F. App'x 384 (6th Cir. 2016).



**Elizabeth E. McGinn** (L) is a partner in the Washington and New York offices of **Buckley Sandler LLP**. She advises clients about the risks related to internal privacy and information security practices as well as the risks related to the use of third-party vendors. She can be reached at emcginn@buckleysandler.com. **James T. Shreve** (C) is counsel at the firm's Chicago office, where he advises clients on privacy, data security and cyber risk issues. He can be reached at jshreve@buckleysandler.com. **Daniel Paluch** (R) is an associate in the firm's Los Angeles office, where he focuses on enforcement and litigation matters. He can be reached at dpaluch@buckleysandler.com.