Your Data Was Stolen, But Not Your Identity (Yet)

Majority consensus grows on the scope of permissible data breach standing

By Kristen L. Burge,
Litigation News
Associate Editor

Photo illustration: Elmarie C. Jara; © iStockphoto

Cyberattack victims can sue data custodians despite not suffering actual identity theft. In determining the plaintiffs' standing, a growing majority of circuit courts now turn to the nature of stolen data to determine whether the victims experience a "substantial risk" of identity theft.

The U.S. Court of Appeals for the Federal Circuit joined the majority approach—followed by the Sixth, Seventh, and Ninth Circuits—holding that victims alleging personal data theft, including medical identification numbers, have standing to pursue their claims.

A minority of circuits, on the other hand, require data breach compromises to include Social Security or credit card numbers before finding a substantial risk exists. In the wake of significant consumer data breaches, the material circuit split signals a need for U.S. Supreme Court intervention to create a uniform test governing standing in consumer data breach cases.

RISK OF IDENTITY THEFT "TOO SPECULATIVE" FOR CERTAIN DATA CATEGORIES

In *Attias v. CareFirst, Inc.*, the U.S. District Court for the District of Columbia addressed whether policyholders had standing to sue following an intentional breach of CareFirst's databases. To issue insurance policies to its customers, CareFirst collects and stores policyholders' personal information, which includes names, birthdates, email addresses, Social Security numbers, and credit card information. CareFirst also assigns a health information identification number to each policyholder. In *Attias*, the policyholders alleged that a data breach compromised this information, thereby creating a risk of future identity theft.

In the cyberattack, a hacker invaded 22 of CareFirst's computers and accessed policyholders' personal information. Shortly after CareFirst announced the breach, seven policyholders sued CareFirst, on behalf of all data breach victims, based on their increased risk for potential identity theft. CareFirst did not dispute that identity theft, should it materialize, would constitute a concrete and particularized injury. Instead, CareFirst argued the risk of future identity theft, based in part on the nature of the stolen data, was not substantial; the policyholders did not allege the hackers accessed Social Security or credit card numbers, and without such information compromised, the threat of identity theft was minimal.

With no actual or imminent harm, CareFirst maintained the policyholders lacked Article III standing—specifically injury in fact. Accordingly, CareFirst filed a motion to dismiss. The district court agreed with CareFirst's position and found the policyholders "had alleged neither a present injury nor a high enough likelihood of future injury." The district court questioned how the policyholders would be subjected to identity theft based on the nature of the information taken (citing the medical identification numbers). Because the alleged theft did not extend to Social Security or credit card numbers, the district court determined the risk of harm was "too speculative." In other words, a compromise of less sensitive personal information did not give rise to an "actual or imminent" harm.

RISK OF IDENTIFY THEFT SUFFICIENT FOR STANDING

The policyholders challenged the district court's ruling that the data breach did not give rise to an actual or imminent harm. On appeal, the U.S. Court of Appeals for the District of Columbia Circuit acknowledged "[n]obody doubts that identify theft, *should it befall one of these plaintiffs*, would constitute a concrete and particularized injury." Instead, the question of the policyholders' standing turned on "whether the complaint plausibly *alleges* that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence." Ultimately finding the allegations sufficient, the court reversed the district court's dismissal for lack of standing.

Citing the applicable test for injury in fact in the seminal decision *Spokeo, Inc. v. Robins*, the D.C. Circuit explained that the policyholders must allege they suffered an injury in fact, which *Spokeo* defines as "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." It is the plaintiff who carries the burden "to make all of these showings . . . , but the burden grows as the litigation progresses." At the pleading stage, the bar is at its lowest. While "self-imposed risk mitigation costs" may support the redressability requirement for Article III standing, the costs associated with the policyholders' responses to a data breach would not by themselves satisfy the injury in fact element.

As a preliminary matter, the D.C. Circuit rejected the conclusion that the policyholders failed to allege theft of their Social Security or credit card numbers. Per the complaint's definitions, the plaintiffs defined the stolen sensitive information collectively to include "patient credit card . . . and social security numbers." Thus, the district court's rationale for concluding the breach presented no substantial risk of identity theft was flawed. The complaint identified the stolen information necessary for hackers to commit financial fraud. This alleged breach placed the policyholders at high risk of identity theft, which constitutes an "actual or imminent harm." Based on this risk, the D.C. Circuit held the policyholders met "the low bar to establish their standing at the pleading stage."

A deliberate hack of personal data, including medical identification numbers, though not as versatile as Social Security or credit card numbers, is sufficient to demonstrate an actual or imminent harm.

Alternatively, even if the breach did not expose the policyholders' Social Security and credit card numbers, theft of health insurance subscriber identification numbers creates a substantial risk of medical fraud. The D.C. Circuit explained that in these cases, victims experience a real risk that such information will be used to access medical treatment and insurance policies. A deliberate hack of personal data, including medical identification numbers, though not as versatile as Social Security or credit card numbers, is sufficient to demonstrate an actual or imminent harm. "Why else would hackers break into a . . . database and steal consumers' private information?" asked the appellate court. "Presumably, the purpose of the hack is, sooner or later, to make fraudulent

charges or assume those consumers' identities." Stealing one's medical identification, at the very least, gives rise to a plausible allegation of future identity theft.

CIRCUITS SPLIT OVER WHAT STOLEN DATA CREATE IMMINENT HARM

"There is already a well-developed circuit split, and data breaches are likely to continue growing in both frequency and the volume of data," observes Tyler G. Newby, San Francisco, CA, cochair of the ABA Section of Litigation's Privacy & Data Security Committee. A majority of circuits reason that "there is a 'certainly impending' threat that the affected individuals will be the victims of financial or identity fraud. After all, the motive of the hackers is to use the stolen information for their own benefit or to sell it to others," explains Newby. These circuits apply common sense to data breach cases, Newby suggests. "The entire purpose of hacking a company to swipe thousands of credit card numbers or personal identifiers is to misuse that information for gain, like making fraudulent purchases or engaging in tax refund fraud or identity fraud. Why should the people whose information was compromised have to wait until that happens before getting some relief?" asks Newby.

Other Section of Litigation leaders agree. "Identity theft is a big deal that seriously worries anyone potentially affected. These circuit courts are rising to the challenge by increasingly recognizing that privacy rights are real, violations are a real injury, and standing to sue exists," observes Fabrice N. Vincent, San Francisco, CA, cochair of the Section's Class Actions & Derivative Suits Committee. Quoting the Sixth Circuit's opinion in *Galaria v. Nationwide Mutual Insurance Co.*, Vincent explains that while "it might not be 'literally certain' that Plaintiffs' data will be misused, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable. Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security."

"Where a data holder's negligence causes data/privacy breaches that pose material threats of identity theft or potential publicity over private issues like medical care, the consumer suffers real emotional harm (even if the worrisome consequence never comes to pass)," explains Vincent. "That harm ought to be compensable and actionable, just as it is under common-law torts like negligent infliction of emotional distress," he continues. "Such breaches are extraordinarily serious, potentially affecting every aspect of the victim's life. Judicial remedies are certainly merited and absolutely required," concludes Vincent.

The Second, Fourth, and Eighth Circuits, however, more narrowly interpret imminent harm in data breach cases. These courts reject the notion that an increased risk of future identity theft is sufficient to confer standing. These circuits consider the passage of time between the breach and the standing challenge in determining whether there is an "imminence of harm." The longer a victim goes without suffering actual identity theft, the less likely one will suffer an injury, these courts reason.

"Where a data holder's negligence causes data/privacy breaches that pose material threats of identity theft . . . , the consumer suffers real emotional harm (even if the worrisome consequence never comes to pass)."

In these circuits, "the likelihood of injury to any one person whose information was stolen in a data breach is too attenuated to satisfy the Supreme Court's 2013 ruling in *Clapper v. Amnesty International USA* that the threat of injury be 'certainly impending,'" explains Newby. "Instead, these circuits have required plaintiffs to allege some indicia that their information *is* being used in a way that harms them, such as fraud or identity theft," describes Newby. Though certainly setting a higher bar for standing, these circuits "are not permanently locking the federal courthouse doors to persons whose information was compromised through a breach. They are simply requiring them to wait until they experience actual injury, if they ever do," observes Newby.

With the stakes so high, litigating standing in data breach cases remains front and center in consumer litigation. With the division among the circuits over what constitutes a substantial risk of harm, litigation is sure to continue and is likely to end up before the Supreme Court, predicts Newby. And when it does, "its analysis should address whether a plaintiff has adequately identified particular categories of information that are likely to lead to harm," suggests Newby.

"The question of the threat or imminence of injury from a security incident should turn on the type of data that was compromised," Newby opines. For instance, when stolen data are "sensitive information that can readily be exploited for gain, like financial account numbers and credentials, login credentials and passwords to e-commerce sites or email accounts, Social Security numbers, drivers' license numbers, and similar information, the likelihood that the information is going to be misused is high," observes Newby. "But the same cannot be said for information that is generally available, like names, birthdates, and email addresses (without login credentials)," says Newby. "If data can be accessed publicly, such as a person's email address, home address, telephone number, or birth date, how does the compromise of that information cause a certainly impending injury?" he argues.

But "reality is that most, if not all, of these cases settle before trial. Apportioning settlement funds among those who never suffered any consequences from a breach may ultimately dilute the remedies available to those who did experience real difficulties," Newby concedes.

Drawing on public policy, Vincent advocates the nature of the data breached should inform damages and the remedy, not dictate access to the courts. "Only such a system will properly motivate the data holder to take the steps necessary to prevent data breaches as well as to offer real solutions to data breaches that have already occurred," suggests Vincent. "In a perfect world, all compromised persons would have standing to sue, and the severity of the breach, e.g., the importance of the compromised data and likelihood or actuality of ensuing further harm, would inform the magnitude

of recoverable damages/remedy analysis (instead of a harsh standing rule that can unfairly bar claims in the first instance)," maintains Vincent.

ADVICE TO LITIGATORS NAVIGATING THE CIRCUIT SPLIT

In the wake of nationwide data breaches, litigators must heed the various circuits' nuanced standing analyses. Where parties litigate a case largely determines whether a threat of future identity theft confers standing and, in turn, determines the recourse available to data breach victims.

To that end, Section leaders provide some guidance. For plaintiffs' attorneys, class representative and venue selection are critical. "In the circuits that apply the narrower Article III standing, plaintiffs' lawyers will need to find named plaintiffs that have experienced some indicia of fraud using their stolen credentials to get their cases past the pleading stage," advises Newby.

Alternatively, "plaintiffs' counsel may focus their efforts on identifying and representing class representative plaintiffs who reside in circuits that apply the more permissive Article III standard, such as the Sixth, Seventh, or Ninth Circuits, each of which has major population centers," says Newby. Because some courts consider the time between the data breach and a standing challenge relevant to the "imminent harm" analysis, plaintiffs' attorneys should not delay filing suit.

As for the defense bar, "defense lawyers may consider whether a standing challenge is really the best strategy to resolve the case," warns Newby. In circuits applying the more permissive bar to standing, a challenge is less likely to succeed. Also, counsel should be aware that "Article III applies only to federal courts, and some states have much broader standing requirements," Newby cautions. "Even so, in most cases, defendants will prefer to be in federal court to state court," notes Newby. All told, defense attorneys should not forget the plaintiff's burden to establish injury in fact increases as the case progresses. If discovery reveals that no identity theft materialized, defendants may want to consider reviving their standing challenge.

Regardless of venue, attorneys should recognize "representation of plaintiffs who actually experienced some fraud following the security incident will be strong protection against a standing challenge, no matter where the plaintiff resides," Newby concludes.

RESOURCES

- *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017), available at http://bit.ly/LN432-attias.
- *Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193 (D.D.C. 2016), available at http://bit.ly/LN432-attias2.
- *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), available at http://bit.ly/LN432-spokeo.
- *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016), available at http://bit.ly/LN432-galaria.
- *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013), available at http://bit.ly/LN432-clapper.
- Sean Fernandes, "Fourth Circuit Weighs in on Data Breach Standing," *Privacy & Data Sec.*, Feb. 15, 2017, available at http://bit.ly/LN432-fernandes.
- Robert T. Denny, "Data Breach Plaintiffs Alleging Future Harm Clear Standing Hurdle," *Litigation News*, Jan. 11, 2016, available at http://bit.ly/LN432-denny.
- Heidi J. Milicic, "Standing to Bring Data Breach Class Actions Post-*Clapper*," *Com. & Bus. Litig.*, Aug. 7, 2014, available at http://bit.ly/LN432-milicic.