Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

9th Circ.'s Zappos Ruling Leaves Data Breach Standing Fuzzy

By **Allison Grande**

Law360 (March 19, 2018, 6:16 PM EDT) -- The Ninth Circuit this month added to the confusion over whether theft of consumer data is enough to establish Article III standing in the wake of two landmark U.S. Supreme Court rulings, reviving privacy claims brought by a group of consumers after a massive data breach at Zappos.com affected 24 million shoppers.

In light of the high court's landmark rulings in Clapper v. Amnesty International and Spokeo v. Robins, federal appeals courts have come to sharply different conclusions on the issue of whether data theft alone is sufficient to establish an actual and imminent injury.

The Ninth Circuit offered the latest data point in a March 8 ruling that revived privacy claims brought by a putative class of Zappos.com Inc. customers following a 2012 data breach. That conclusion came down on the side of the D.C., Sixth and Seventh circuits, which embraced the premise that a risk of future harm stemming from the theft of consumer data is enough for standing. The Second, Third, Fourth and Eighth circuits each have ruled the opposite way in similar data breach disputes.

"I think the only solid pattern forming is one of uncertainty" when it comes to the question of "whether a breach plus a mere risk of harm — without an out-of-pocket financial loss — is enough to create standing," said Shook Hardy & Bacon LLP data security and privacy group chair Al Saikali.

The debate over whether consumers have standing in these types of disputes has intensified in light of the Supreme Court's 2013 ruling in Clapper that injuries must be real or imminent and not merely speculative, followed up with the 2016 Spokeo decision that harm must be concrete and mere statutory violations do not suffice.

The question is whether plaintiffs whose personal information has been stolen by criminal hackers, but who haven't yet suffered identity theft or other tangible injuries, should be allowed to proceed with claims such as negligence and alleged contractual violations.

"It's somewhat analogous to toxic tort situations," Axinn Veltrop & Harkrider LLP partner Thomas Rohback said. "There's been an exposure, and the question is if and when the symptoms are going to manifest themselves."

To help bolster their claims, plaintiffs have increasingly been arguing that they face a sufficiently imminent risk of future harm because hackers' main motivation is to use the data they steal for illegal purposes — an argument endorsed by the Ninth Circuit in reviving the Zappos litigation.

"Courts are recognizing that these breaches cause real and not hypothetical injuries. But that does not mean that a plaintiff has to allege that he or she is already the victim of identity theft to sufficiently allege standing. Like the D.C. Circuit in CareFirst recognized, hackers steal information for the purpose of committing fraud," said plaintiffs' attorney Amy Keller of DiCello Levitt & Casey LLC, who is currently serving as co-lead counsel for plaintiffs in sprawling litigation over the massive data breach at Equifax that compromised more than 148 million consumers' personal data.

Attorneys don't expect this wave to recede any time soon, with Keller predicting more judges will "continue to become more appreciative of the value of data and what it means when the data isn't safeguarded."

"In some instances, the type of data that is compromised in these breaches is difficult to or cannot be changed, and its exposure is likely to impact consumers for a very long time," Keller said.

Alexander Bilus, the co-chair of Saul Ewing Arnstein & Lehr LLP's cybersecurity and privacy practice, agreed that courts in the coming years are likely to become "more receptive" to allowing these types of data breach claims through the door, as the plaintiffs' bar continues to refine its arguments and the frequency of data breaches leads to a greater appreciation for the value of data.

"With this Ninth Circuit decision and with the general greater understanding that courts and the American population have about the dangers of data breaches and the fact that they seem to be becoming more widespread and in some circumstances bigger, people in some way are beginning to have a better understanding of the harm that could come from them," Bilus said.

Such a shift would only serve to further the divide between jurisdictions that are willing to embrace this harm argument and those that require identity theft to already have occurred when plaintiffs show up at the courthouse — a debate that many argue won't be settled until the Supreme Court definitely weighs in.

"Courts will continue to struggle on whether a data breach is a signal that a company did something wrong or is itself a victim and should not be further burdened with litigation," Troutman Sanders LLP partner Ron Raether said.

The Supreme Court recently had the chance to tackle the emerging divide when CareFirst urged review of the D.C. Circuit's finding that policyholders suing over a 2014 data breach had “cleared the low bar to establish their standing at the pleading stage” by asserting there was a substantial risk their stolen personal information could be used “for ill" purposes such as identity theft, even though it had yet to be misused.

But the justices in February declined to take up that opportunity, a decision attorneys said was likely attributable to several factors, including the possibility that the Supreme Court is waiting for the data breach landscape to

become better developed and establish a better understanding of the potential consequences of such intrusions.

"My best guess is that the Supreme Court chose not to take up the split because they wanted the law to develop further and more courts to weigh in on the issue," Saikali said. "But it's also possible that the Supreme Court chose not to weigh in because this is an area of litigation that is changing very quickly, as is the underlying technology that results in the lawsuits, so they may be waiting for the area to 'settle' further before weighing in."

While the emergence of more breaches could lead more courts to the conclusion endorsed by the Ninth Circuit that these incidents are inherently harmful events, a wider sample size could also potentially lead to the opposite result, attorneys say.

"What might affect this type of litigation is if there are some sort of studies done to really ascertain how many cases of identity theft there are for every breach," Mayer Brown LLP partner Donald Falk said. "Obviously, data breaches are a real problem and people are severely injured by identity theft, but when there are millions of sets of personally identifiable information breached, we're not seeing millions of cases of identity theft, so there's something out of whack there."

The proliferation of data breaches could also make it more difficult for plaintiffs to tie the identity theft they suffered to a particular incident, further complicating the harm analysis for courts.

"The question for courts is likely to be, what happens when a defendant comes back and says this plaintiff's information has been breached three other times — how do we know that this particular breach led to identity theft?" Bilus said. "That may be another factor pushing courts to say at the pleading stage that it's enough ... that plaintiffs have been subject to a breach and not tie it to any actual identity theft because otherwise it might be impossible for plaintiffs to ever recover."

As the circuit courts continue to go opposite ways on these issues, and until the Supreme Court weighs in, the fates of both parties are likely to primarily depend on the jurisdiction in which they find themselves, attorneys noted. But, as Keller pointed out, court decisions are nuanced, and details like the size and scope of an incident could tip the scales.

"It's important for plaintiffs' attorneys to really understand the scope of the breach and damages that could occur," Keller said. "These cases will largely rise and fall on the types of data allegedly stolen."

Being in tune with the specifics of the breach could help both sides reach different results in circuits that may have gone against them in the past, attorneys noted.

For example, the Ninth Circuit panel gave great weight to the sensitivity of the information stolen in the breach, which included credit card numbers that can be used to commit identity theft; the fact that some plaintiffs had alleged actual identity theft; and the heightened risk of harm that plaintiffs faced not at the present moment, but when they filed their complaint on the day Zappos disclosed the breach.

But the conclusion may be different in a situation where the exposure of data resulted from a lost laptop or a security vulnerability that has been identified but not necessarily exploited, or when less sensitive information that isn't hard to change or closely linked with identity theft is compromised, attorneys noted.

"It may come to the point where different types of data have different lifetimes of non-speculative harm," Falk said.

While courts sort out the standing issues, companies can take steps on their own to help minimize exposure, attorneys say. Given that the vast majority of these cases turn on claims that companies were negligent in failing to adequately protect consumer data, striving to put in place the most robust data security possible could help to stave off litigation, especially as it moves past the threshold question of standing.

"The best defense is going to be a good offense," Bilus said. "Even if plaintiffs get past standing, defendants should still have very strong arguments to make in their favor if they're doing the right things to protect data."

The plaintiffs in the Zappos case are represented by Douglas Gregory Blankinship of Finkelstein Blankinship Frei-Pearson & Garber LLP.

Zappos is represented by Stephen J. Newman of Stroock & Stroock & Lavan LLP.

The case is Theresa Stevens et al. v. Zappos.com Inc., case number 16-16860, in the U.S. Court of Appeals for the Ninth Circuit.

--Editing by Philip Shea and Kelly Duncan.