Legal Backgrounder

Vol. 33 No. 7 May 4, 2018

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

# Ninth Circuit's Flawed *Zappos* Decision Is Cautionary Tale for Corporate Victims of Cyberattacks

by Michelle Visser and David Cohen

As the well-known proverb provides, "no good deed goes unpunished." On March 8, 2018, the U.S. Court of Appeals for the Ninth Circuit unfortunately lent support to that theory when it reversed dismissal of a consumer data-breach class action against online retailer Zappos.com (Zappos), a victim of a cybersecurity breach, in part because Zappos recommended after the breach that its customers whose personal information was compromised change their passwords. According to the Ninth Circuit, Zappos' recommendation was effectively an admission that its customers faced a risk of fraud from the breach that was sufficient to give them standing to sue under Article III of the U.S. Constitution. The *Zappos* decision highlights a growing split among courts of appeals as to whether a corporate cybersecurity-breach victim's efforts to assist its customers in the wake of the breach should weigh in favor of those customers' standing to sue.

## Standing in Federal Court Based on Future Harm

A private plaintiff seeking to invoke the federal courts' jurisdiction must satisfy the standing requirements of Article III, under which a plaintiff must allege and ultimately prove, among other things, an "injury in fact." As the Supreme Court has explained, to show an injury in fact, a plaintiff must demonstrate an injury that is "(a) concrete and particularized" and "(b) actual or *imminent*, not conjectural or hypothetical." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (emphasis added). Constitutional standing also requires the plaintiff to show "traceability," *i.e.*, a causal connection between the injury alleged and the conduct complained of, as well as "redressability," *i.e.*, that a judicial decision would redress his or her injury. *Id. at 560*–61.

In the context of data security breaches, lower courts have reached differing conclusions as to whether the risk of fraud or identity theft from the breach created a sufficiently "imminent" injury for standing purposes.[1] (The Supreme Court has not directly addressed the issue.) In 2010, the Ninth Circuit held that it did, reasoning that "[i]f a plaintiff faces a credible threat of harm, and that harm is both real and immediate, not conjectural or hypothetical, the plaintiff has met the injury-in-fact requirement for standing under Article III." *Krottner*, 628 F.3d at 1143. Applying that standard, it concluded that plaintiffs alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data,

[1] *Compare, e.g., Attias v. Carefirst, Inc.*, 865 F.3d 620, 630 (D.C. Cir. 2017)(standing conferred); *Galaria v. Nationwide Mut. Ins.*, 663 F. App'x 384, 387–91 (6th Cir. 2016)(standing conferred); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966–70 (7th Cir. 2016)(standing conferred); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692–93 (7th Cir. 2015)(standing conferred); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010)(standing conferred), *with In re Supervalu, Inc.*, 870 F.3d 763, 769–72 (8th Cir. 2017)(standing denied); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90–91 (2d Cir. 2017)(standing denied); *Beck v. McDonald*, 848 F.3d 262, 273–76 (4th Cir. 2017)(standing denied); *Reilly v. Ceridian*, 664 F.3d 38, 41–46 (3d Cir. 2011)(standing denied).

**Michelle Visser** is a Partner, and **David Cohen** is Counsel, with Ropes & Gray LLP in the firm's San Francisco, CA and New York, NY office, respectively.

and that they therefore adequately pleaded Article III standing. *Ibid.*

Subsequently, in *Clapper v. Amnesty International*—a case outside of the cybersecurity-breach context—the Supreme Court held that where a plaintiff contends that harm is imminent but has not yet occurred, the harm must be "certainly impending" in order to constitute an injury in fact. 568 U.S. 398, 410 (2013). The *Clapper* Court also noted that in limited circumstances, it had also found standing based on a "substantial risk" of harm, but it did not state whether the "substantial risk" standard is distinct from the "certainly impending" standard. *See id.* at 414 n.5; *see also Susan B. Anthony List v. Driehaus,* 134 S. Ct. 2334, 2341 (2014).

Regardless of the standard used, *Clapper* made crystal clear that a "speculative chain of possibilities" or "speculation about the decisions of independent actors" not before the Court will not give rise to standing. *Clapper*, 568 U.S. at 409, 414 & n.5. Thus, in *Clapper,* the Court denied standing to several attorneys and human rights, labor, legal, and media organizations who claimed their communications with foreign intelligence targets might be intercepted by the government under a portion of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a.

The interception would only have occurred if the government actually decided to target plaintiffs' non-U.S. contacts, did so under § 1881a, obtained approval from a special court, succeeded in intercepting the communications, and plaintiffs were parties to those particular communications. This, the Court held, was the quintessential "speculative chain of possibilities" that cannot give a plaintiff standing. And, plaintiffs' theory impermissibly rested on "speculation about the decisions of independent actors," such as the special court.

In *Zappos*, the Ninth Circuit was tasked with determining whether its holding in *Krottner* remained good law in the wake of *Clapper*, and if so, whether *Krottner* compelled a finding that the consumer plaintiffs suing over Zappos's security breach had standing.

## The *Zappos* Decision

In 2012, hackers allegedly broke into Zappos' computer network and stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than 24 million Zappos customers. Zappos emailed its customers to notify them of the attack and recommended that they reset their Zappos.com account passwords and change the passwords "on any other web site where [they] use the same or a similar password." Several of the customers then brought class actions against Zappos, with some asserting they had already suffered losses from fraudulent use of their data as a result of the breach and others merely alleging that they faced an increased "risk" of fraud from the breach.

The U.S. District Court for the District of Nevada held that the plaintiffs who alleged losses from actual misuse of their data had Article III standing, but that the plaintiffs who alleged a mere risk of fraud did not. After the plaintiffs who allegedly suffered misuse voluntarily dismissed their claims, the "risk of harm" plaintiffs appealed to the Ninth Circuit.

The Ninth Circuit panel reversed the district court on the "risk of harm" claims, holding that the plaintiffs pled a risk of future harm that was sufficient to give them standing. The court began by concluding that *Clapper* did not overrule *Krottner*, but rather simply reached a different result because the allegation of possible future harm in *Clapper*, unlike in *Krottner,* relied on a "speculative multi-link chain of inferences."

The *Zappos* panel then held that *Krottner* compelled a finding that the *Zappos* plaintiffs had standing. Just as in *Krottner*, said the Ninth Circuit, the *Zappos* plaintiffs alleged a "credible threat" of harm because the "information taken in the data breach" gave "hackers the means to commit fraud or identity theft."

Notably, the Ninth Circuit supported its conclusion in part by pointing to Zappos' own efforts to assist its customers after the breach: it reasoned that "Zappos itself effectively acknowledged" the risk of identity theft or fraud "by urging affected customers to change their passwords on any other account where they may have used the same or similar password." The court also rejected Zappos' argument that the passage of several years without any reported misuse on the "risk of harm" plaintiffs' accounts undermined their claim of imminent harm, reasoning that this argument raised a factual issue concerning the risk of harm that could not be resolved on the pleadings.

## Analysis

The *Zappos* decision is vulnerable to being overruled because it runs afoul of the bedrock principle, confirmed in *Clapper*, that Article III standing cannot be premised on a "speculative chain of possibilities" or "speculation about the decisions of independent actors" not before the court. Just as the possible approval of surveillance by the third-party special court in *Clapper* was too unpredictable to allow standing, the actions of a third-party hacker or other criminal are likewise unpredictable.

Even if the hacker has the ability to commit fraud, which is not always the case, he may not have the intent to commit fraud, for any number of reasons. In fact, hackers' avowed purposes often are not to commit identity theft or harm consumers, but rather to embarrass or harm the hacked corporation, steal trade secrets, or make a political statement.

What is more, it is typically not the *hacker himself* who misuses stolen data—instead any misuse is committed by downstream criminals who must first purchase the data on the black market. Thus, only *if* the hacker decides to sell the data, and *if* third parties become aware of the stolen information, and *if* they reveal their interest in it, and *if* they actually take steps to acquire and use the information to plaintiffs' detriment, and *if* they are successful in doing so, and *if* plaintiffs suffer actual damage from the misuse, then and only then will plaintiffs suffer any injury from the breach. There are just as many "ifs" in this scenario as there were in *Clapper*.

Moreover, even if the plaintiffs had adequately pleaded that harm from purportedly stolen data is sufficiently likely, they were required to plead facts showing that the harm is "imminent," *i.e.*, it will occur immediately, if at all. *See, e.g., Lujan*, 504 U.S. at 560 (injury must be "actual or imminent"). The complaint's failure to allege that the plaintiffs at issue on appeal had experienced any misuse undercuts their claim that harm from the 2012 breach was imminent.[2]

Even more troubling is the *Zappos* panel's reliance on Zappos' efforts to assist its customers in the wake of the breach to support plaintiffs' standing. Several other decisions have used similar reasoning.[3] These holdings overstate the probative value of statements or offerings like these in the wake

[2] *See, e.g., Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017)("'[A]s the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative."); *Duqum v. Scottrade, Inc*., No. 15-cv-1537, 2016 WL 3683001, at *4 (E.D. Mo. July 12, 2016)("[A]s more time lapses without the threatened injury actually occurring, the notion that the harm is imminent becomes less likely.").

[3] *See Remijas*, 794 F.3d at 694 (in holding that the consumers adequately pleaded standing, treating company's offer of credit monitoring and acknowledgement of 9,200 fraudulent charges as an admission that consumers


ISBN 1056 3059

of a breach, which are often made in an abundance of caution, to generate goodwill, and/or to minimize regulatory enforcement risk. Nearly every state, for example, requires companies to notify consumers of certain data security breaches, and regulators have long pressed such companies to offer identity theft prevention or mitigation services as well, even where those services may not address the specific risks, if any, presented by the breach at hand. Those pressures are only increasing: a recent Connecticut statute requires companies to provide "appropriate identity theft prevention services and, if applicable, identity theft mitigation services" in the context of certain breaches. Conn. Gen. Stat. § 36a-701b. And California provides that a company that is obligated under its breach notification statute to notify consumers of a breach of only online credentials may comply with the statute by sending a notice by electronic or other means directing the consumers to change those credentials. Cal. Civ. Code § 1798.82(j)(4).

More importantly, the holdings by the *Zappos* court and courts using similar reasoning will discourage companies from taking steps to help their customers minimize the risk of misuse in the wake of a security breach when offering such assistance is not legally required. For this reason, several courts have expressly refused to use corporate data-breach victims' statements against them when evaluating standing.[4]

**Conclusion**

The Supreme Court should overrule the *Zappos* decision at its earliest opportunity. In the meantime, companies litigating within the Ninth Circuit on similar facts should keep in mind that they may have potentially powerful alternative defenses to the "risk of harm" theory tied to Article III standing, including that a "risk of harm" is generally not an actionable damage under the causes of action data breach plaintiffs typically press, *see, e.g. In re Yahoo! Inc. Cust. Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2018 WL 1243332, at *9 (N.D. Cal. Mar. 9, 2018), and that plaintiffs using the same or similar passwords across different websites may be barred from or limited in recovering by reason of their having been at fault.[5]

faced a sufficient risk of harm); *Lewert*, 819 F.3d at 967 (citing company's suggestion that its customers check their "credit reports" in the wake of a breach in concluding that plaintiffs had standing for purpose of motion to dismiss).

[4] *See, e.g., Beck,* 848 F.3d at 276 ("Contrary to some of our sister circuits, we decline to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals. To adopt such a presumption would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit."); *In re Horizon Healthcare Servs. Data Breach Litig.*, 846 F.3d 625, 634 n.12 (3d Cir. 2017)("We agree with Horizon that its offer should not be used against it as a concession or recognition that the Plaintiffs have suffered injury. We share its concern that such a rule would 'disincentivize[] companies from offering credit or other monitoring services in the wake of a breach.'"). Those refusals are consistent with the policy objectives underpinning other areas of the law that analogously seek to avoid discouraging beneficial behavior. *See, e.g.*, Fed. R. Evid. 407–08 (subsequent remedial measures and compromise offers inadmissible to prove negligence or culpable conduct); *cf.* Leonard et al., New Wigmore: A Treatise on Evidence § 7.8 (2d ed. 2017)(noting courts that have adopted privileges to protect against discoverability of medical staff reviews in wake of healthcare accidents and against discoverability of environmental audits).

[5] *See e.g.,* Steve Bellovin, *Password Compromises*, Fed. Trade Comm'n (Sept. 19, 2012, 12:18 PM) https://www.ftc.gov/news-events/blogs/techftc/2012/09/password-compromises ("The single most important defense" to password compromises "is to avoid reusing passwords"); Dan B. Dobbs, Paul T. Hayden & Ellen M. Bublick, Dobbs' Law of Torts § 218 (2d ed. 2017)(discussing effect of plaintiffs' fault on tort claims).