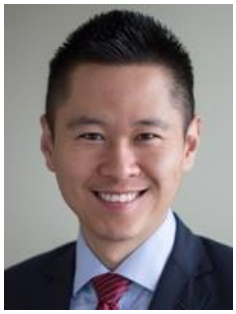
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

9th Circ.'s Expansive Standard For Standing In Breach Case

By **Nathanial Wood and Brandon Ge** (April 6, 2018, 12:16 PM EDT)

Nathanial Wood



Brandon Ge

A recent decision by the U.S. Court of Appeals for the Ninth Circuit illustrates why companies that have experienced a data breach need to closely examine the language of their breach notifications to ensure they are not inadvertently increasing their litigation risk by unnecessarily suggesting consumers face harm from the incident.

On March 8, 2018, the Ninth Circuit revived claims related to a 2012 data breach affecting the internet retailer Zappos.com Inc., holding that the plaintiffs sufficiently established Article III standing based merely on the future risk of identity theft, regardless of whether the plaintiffs suffered actual harm. In doing so, the court pointedly relied on Zappos' breach notice as evidence that the putative class was at a heightened risk for fraud and identity theft, despite the fact that they had not actually suffered any such harm in the years since the breach occurred.

The court's decision also furthers a circuit split on the issue of whether consumers can file suit in federal court when they haven't suffered any concrete harm from the breach. The decision is likely to drive plaintiffs attorneys to seek to file cases in the Ninth Circuit and increase the circuit's already high volume of data breach litigation.

Background

At issue in the case, In re Zappos.com Inc., was whether the plaintiffs had Article III standing to bring claims based on a January 2012 data breach where hackers breached Zappos' servers and allegedly 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. Affected customers filed putative class actions around the country, claiming that Zappos failed to adequately protect their personal information.

While one group of plaintiffs in the class action alleged that the hackers actually conducted financial transactions using the stolen information, the plaintiffs at issue in this appeal did not allege any actual injury. Instead, they based their standing primarily on the risk that the Zappos hackers might use the information to commit identity theft, including a higher risk of "phishing" and "pharming," methods hackers can use to exploit available information and obtain more personally identifiable information.

Supreme Court vs. Ninth Circuit Views on Standing

In order to pursue their claims, the plaintiffs had to get around the U.S. Supreme Court's 2013 decision in Clapper,[1] which set an arguably high bar for establishing standing in cases where there was only fear of future harm. In Clapper, the plaintiffs challenged surveillance procedures authorized by the Foreign Intelligence Surveillance Act of 1978, arguing that they had Article III standing based on an "objectively reasonable likelihood" that their communications would be acquired under the statute in the future. The Supreme Court rejected this argument, determining that the plaintiffs' alleged injury was too speculative to meet the threshold of a "certainly impending" injury. Since the decision was issued, numerous data breach cases have been dismissed on the grounds that mere acquisition of the data is insufficient to establish that an injury is "certainly impending."[2]

Here, the plaintiffs sought to circumvent Clapper with the Ninth Circuit's pre-Clapper decision in Krottner,[3] which dealt with a data breach involving Starbucks. In that case, a thief stole a laptop containing the unencrypted names, addresses, and Social Security numbers of approximately 97,000 Starbucks employees. Starbucks sent a letter to affected employees, stating that Starbucks had no indication that the information had been misused, but nonetheless advising them to monitor their financial accounts for suspicious activity and to take appropriate steps to protect against potential identity theft. The only harm that most of the plaintiffs alleged was an "increased risk of future identity theft," but the Ninth Circuit nonetheless held that the plaintiffs had alleged a credible threat of real and immediate harm because a laptop with their personally identifiable information had been stolen.

Naturally, Zappos argued that Krottner was no longer good law in light of the heightened standard announced by the Supreme Court in Clapper. Not so, ruled the Ninth Circuit.

The Ninth Circuit first held that Krottner was still binding unless it was "clearly irreconcilable" with the later Supreme Court decision. The court rejected Zappos' arguments in this regard and found Krottner was not "clearly irreconcilable" with Clapper. The court believed that plaintiffs' alleged injury in Krottner did not rely on a "speculative multi-link chain of inferences," unlike in Clapper. The thief in Krottner had sufficient information to open accounts or spend money at the plaintiffs' expense — which the court considered sufficient regardless of whether the thief knew or cared that such data existed on the stolen computer. In the Ninth Circuit's view, the threat perhaps would have been insufficiently speculative if no laptop had been stolen and the plaintiffs had sued based on the risk that it would be stolen at some point in the future.

In addition, the Ninth Circuit viewed Clapper as different due to its national security implications and because the plaintiffs sought declarations that actions by the executive and legislative branches were unconstitutional. Therefore, the standing analysis was particularly rigorous, unlike in Krottner. The Supreme Court also noted in Clapper that the plaintiffs had not alleged a substantial risk of injury because their theory relied on too many inferences. However, in its 2014 post-Clapper decision, Susan B. Anthony List v. Driehaus, the Supreme Court acknowledged that "[a]n allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk that the harm will occur.'"

The Ninth Circuit also noted the consistency of its determination with post-Clapper decisions in two other circuits holding that a data breach where a hacker targets personally identifiable information sufficiently creates a risk of harm to support standing. In particular, the court cited the D.C. Circuit's decision in Attias v. CareFirst Inc.[4] and the Seventh Circuit's decision in Remijas v. Neiman Marcus

Group LLC[5] as support for determining that a plaintiff can sufficiently demonstrate a substantial risk of harm simply because a hack occurred—ostensibly, the purpose of any hack is to make fraudulent charges or commit identity theft. The citation to Remijas is particularly telling with respect to the Ninth Circuit's views on data breach cases, as it cited the language from the Seventh Circuit's decision which essentially assumed that all cyberattackers intend to steal data to make fraudulent charges or commit identity theft, contrary to the reality in numerous cyber intrusion matters that no unauthorized charges or identity theft results from the incident.

The Ninth Circuit Applies Its Expansive View of Standing in Zappos

Having decided that it could effectively ignore Clapper, the Ninth Circuit then determined that Krottner controlled the result in Zappos because the sensitivity of the stolen data was similar to that in Krottner. Notably, the court made this determination despite the fact that the Zappos breach did not involve Social Security numbers, unlike the Starbucks breach at issue in Krottner. However, as the court noted, the Zappos breach involved credit card numbers, which was not part of the Starbucks breach.

Emphasizing its view of the sensitivity of credit card numbers, the Ninth Circuit pointed to federal legislation prohibiting merchants from printing credit numbers on receipts. The court also held that Zappos had "effectively acknowledged," i.e., admitted, that the stolen data could be used to harm the plaintiffs — a ruling that likely surprised Zappos since it had done nothing more than include fairly standard breach notification language that, as characterized by the court, "urg[ed] affected customers to change their passwords on any other account where they may have used 'the same or a similar password.'" This is especially noteworthy in that the court essentially punished Zappos for seeking to provide guidance to its customers on how to protect themselves.

The court highlighted that other plaintiffs in the case had alleged financial losses due to the Zappos breach, which the court believed undermined Zappos' argument that the information stolen in the breach could not be used for fraud or identity theft. The Ninth Circuit also rejected Zappos' argument that too much time had passed since the breach for the harm to be imminent, instead assessing the standing claims as of when the action was filed in January 2012. Moreover, the court noted that fraud or identity theft can occur years after information is breached.

Lessons Learned

There are several key takeaways from the Ninth Circuit's decision in this case. First, it underscores the continued debate over the applicability of the Supreme Court's standing jurisprudence, as standing continues to be in the "eye of beholder" — as different courts continue to achieve very different results when applying the Supreme Court's ruling in Clapper to data breach litigation. This likely will continue to lead to forum shopping, as plaintiffs seek out friendly jurisdictions for their cases.

Second, the Ninth Circuit's decision may make cases involving credit card information more difficult to defend because the decision accepts that the information involved in the breach — notably, credit and debit card information and passwords — may suffice to allege potential harm, even where Social Security numbers are not involved. The ruling may be used to push the narrative that the mere fact of the breach means the cyberattacker intended to access the information for financial gain — a fact that is belied by the reality that hackers act out of a number of motivations, as evidenced by the U.S. Department of Justice's recent indictment of nine Iranians for hacking into hundreds of universities and corporations to steal intellectual property and academic data (not personal information for identity theft).

Third, the court's decision that standing is to be evaluated as of the filing of the complaint will likely be used by the plaintiffs bar to argue that district courts may not consider post-filing developments, such as the cancellation of credit cards, when determining standing, even in instances in which such motions are being determined years after the breach. But, as noted by the Ninth Circuit, this information would remain relevant for other types of motions, so it does not offer a panacea for plaintiffs that have not suffered any injury.

Fourth, companies should take particular notice of the Ninth Circuit's decision to use Zappos' breach notification as an admission that the breach would potentially lead to consumer harm. Because the Ninth Circuit arguably "punished" Zappos for the warnings in its breach notice, companies should reassess the language in their standard notices to determine whether similar language could be later construed as evidence in favor of a class plaintiff. Given the Ninth Circuit's willingness to rely on such standardized "boilerplate" statements to find standing, companies should be mindful of other communications as well, such as media interviews, press releases, and U.S. Securities and Exchange Commission filings relating to the breach. Such communications should be evaluated in light of this decision and whether any of the language may inadvertently give a plaintiff the proverbial "keys to the courthouse door" by creating standing based on fear of future harm.

The Ninth Circuit's opinion in Zappos demonstrates some courts' willingness to use virtually any documents or communications to evidence a risk of future fraud or identity theft — and perhaps should spark a debate regarding whether companies' notification letters should be permitted to be used in such a fashion, in seeming contravention of long-standing principles that defendants should not be disincentivized from undertaking remedial measures and offering to mitigate potential harm.[6]

Nathanial Wood is a partner in the Los Angeles office of Crowell & Moring LLP. Brandon Ge is an associate in the firm's Washington, D.C., office.

[1] Clapper v. Amnesty Int'l. USA, 568 U.S. 398 (2013).

[2] See, e.g., In re SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763 (8th Cir. 2017) (no standing under Clapper in data breach case where credit card information was allegedly stolen); Whalen v. Michaels Stores, Inc., 689 Fed. Appx. 89 (2nd Cir. 2017) (no standing under Clapper in data breach case where credit card information was stolen and plaintiff alleged that her card information was misused).

[3] Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

[4] Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), cert. denied, No. 17-641, 2018 WL 942459 (U.S. Feb. 20, 2018).

[5] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

[6] See generally Federal Rule of Evidence 407, 409; California Evidence Code § 1152(a) (“Evidence that a person has, ... from humanitarian motives, furnished or offered or promised to furnish money or any other thing, act, or service ... is inadmissible to prove his or her liability for the loss or damage or any part of it.”).