THE
NATIONAL LAW REVIEW

U.S. Supreme Court Allows Zappos Data Breach Litigation to Proceed

Article By Jason C. Gavejian
Joseph J. Lazzarotti Maya Atrakchi
Jackson Lewis P.C. Workplace Privacy Blog

Communications, Media & Internet
Litigation / Trial Practice
9th Circuit (incl. bankruptcy)

Tuesday, March 26, 2019

Yesterday, the U.S. Supreme Court rejected a petition for a writ of certiorari by Zappos requesting the Court to review a Ninth Circuit Court decision which allowed customers affected by a data breach to proceed with a lawsuit on grounds of vulnerability to fraud and identity theft. The ruling stems from a 2012 breach that affected over 24 million Zappos customers, which including hackers accessing customer's names, account numbers, passwords, email addresses, billing and shipping addresses, phone numbers, and the last four digits of the credit cards.

In March of 2018, the Ninth Circuit Court reversed a decision by the United States District Court for the District of Nevada that tossed claims brought by customers affected by the data breach who claimed that the breach left them in "imminent" risk, because they did not allege having already suffered financial losses. A three-judge Ninth Circuit panel held that sensitivity of the information stolen in the breach — including credit card numbers and other means to commit fraud or theft — led them to conclude the customers had adequately alleged an injury. "Plaintiffs allege that the type of information accessed in the Zappos breach can be used to commit identity theft, including by placing them at higher risk of 'phishing' and 'pharming,' which are ways for hackers to exploit information they already have to get even more PII," the panel wrote.

Businesses facing class action litigation following a data breach have long waited for the Supreme Court to weigh in on the issue of whether a demonstration of actual harm is required to have standing to sue. Federal circuit courts over the past few years have struggled with this issue, in large part due to lack of clarity following the U.S. Supreme Court's decision in *Spokeo, Inc. v. Robins* which held that even if a statute has been violated, plaintiffs must demonstrate that an "injury-in-fact" has occurred that is both concrete and particularized, but which failed to clarify whether a "risk of future harm" qualifies as such an injury. For example, the 3rd, 6th, 7th, 9th and D.C. circuits have generally found standing, while the 1st, 2nd, 4th and 8th circuits have generally found no standing where a plaintiff only alleges a heightened "risk of future harm".

In its appeal to the Supreme Court, Zappos argued that "the factual scenario this case presents – a database holding customers' personal information is accessed, but virtually no identity theft or fraud results – is an increasingly common one". The rejection by the Supreme Court of the Zappos petition is considered a setback for companies facing similar litigation. Moreover, the California Consumer Privacy Act, set to take effect in 2020, authorizes a private cause of action against a covered business for damages resulting from a failure to implement appropriate security safeguards which result in a data breach, and the Illinois Supreme Court recently held that actual harm was not required to sue under the Illinois Biometric Information Privacy Law ("BIPA"). The Supreme Court did not provide a reason for its denial of the Zappos petition, nonetheless its decision coupled with these state initiatives, is likely to have a significant impact on data breach class action lawsuits going forward.

Source URL: https://www.natlawreview.com/article/us-supreme-court-allows-zappos-data-breach-litigation-to-proceed