CATEGORIES

- Corporate Governance
- Employment/Workplace Privacy
- Global/Transborder Privacy
- In the News
- Insurance
- Legal Ethics
- Life Sciences/Healthcare
- Litigation
- Marketing & Consumer Privacy
- Policy/Legislation
- Privacy Regulation

INDUSTRIES

- Consumer Products
- Financial Services
- Higher Education
- Law Firms
- Media, Entertainment & Sports
- Secondary Education
- Tax-Exempt Organizations
- Technology

SEARCH BLOG

Search

FOLLOW US

Blog Digest
Twitter
LinkedIn
RSS Feed

Ninth Circuit Wades into Growing Debate over Data Breach Standing

Categories: Litigation, Marketing & Consumer Privacy

by Peter A. Kurtz and Craig A. Newman on March 26, 2018

SHARE THIS PAGE:

Is the risk of future harm enough to satisfy Article III standing in a data breach suit? That's the question courts of appeals around the country are wrestling with now – and reaching opposing results. The U.S. Court of Appeals for the Ninth Circuit is the latest to wade into this debate on data breach standing in its recent opinion, *In re Zappos.Com, Inc., Customer Data Security Breach Litigation*.

In re Zappos concerned a data breach of the online retailer Zappos.com. Hackers allegedly stole the personal identifying information of more than 24 million Zappos customers, including their names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information. In the consolidated class-action lawsuit that followed the breach, the trial court rejected the claims of many plaintiffs, finding they had no Article III standing to sue because they had not suffered an actual injury. No one had used their personal information to commit fraud or identity theft.

On appeal, the Ninth Circuit disagreed with the trial court's analysis. The court ruled that the plaintiffs could establish standing even if they had not yet suffered an actual injury because the breach put the plaintiffs at a substantial risk of future harm. That risk was substantial, according to the court, because of the type of information stolen in the breach. The court explained that credit card numbers and other sensitive information useful for "phishing" and "pharming" attacks gave hackers the means to commit fraud or identity theft. The court also noted that other Zappos customers, whose information was also exposed but whose standing to sue was not at issue in *In re Zappos*, had suffered financial losses because of the data breach. This was further evidence that the plaintiffs in the suit could still be harmed.

It did not take long for parties in other data breach suits to notice *In re Zappos*. Eight days after the opinion issued, plaintiffs in *Antman v. Uber Technologies, Inc.*, cited it in arguing they had standing to sue. That case, in federal district court in Northern California, concerns a 2014 data breach of Uber drivers' personal identifying information, including their Social Security numbers. The plaintiffs alleged that, even if they had not yet suffered an injury, they still had standing because the disclosure of their Social Security numbers put them at risk of future harm.

We'll have to wait to see how the court rules in *Antman*. No doubt other courts will soon weigh in, too, on this important and developing area of law.

Peter A. Kurtz
Associate
212-336-2068
Email

Craig A. Newman
Partner
212-336-2330
Email

Next ›

1133 Avenue of the Americas New York, New York 10036 | Tel: 212.336.2000