

CLIENT ALERT

Ninth Circuit Revives Data Breach Class Action, Finds Risk of Identity Theft Without Actual Harm Sufficient to Establish Standing

March 12, 2018

On March 8, 2018, the U.S. Court of Appeals for the Ninth Circuit revived claims related to a 2012 data breach affecting the internet retailer Zappos.com, holding that the plaintiffs sufficiently established Article III standing based on the future risk of identity theft, regardless of whether the plaintiffs suffered actual harm. Given the number of cases filed in the Ninth Circuit, this decision is likely to have a significant impact on data breach litigation. The various circuits are currently split on the standard for establishing Article III standing in data breach litigation, a split that will likely continue until the Supreme Court addresses the issue.

At issue in the case, *In re Zappos.com*, was whether the plaintiffs had Article III standing to bring claims based on a January 2012 data breach where hackers allegedly stole the personal information of more than 24 million Zappos.com Inc. (Zappos) customers—names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information. While a 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.

In deciding the case, the Ninth Circuit relied on its 2010 ruling in *Krottner v. Starbucks Corp.*, where it held that various Starbucks employees had alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data. In relying on *Krottner*, the Ninth Circuit rejected Zappos' argument that *Krottner* is no longer good law after the Supreme Court's decision in *Clapper v. Amnesty International USA*, determining instead that *Krottner* is not clearly irreconcilable with *Clapper* and therefore remains binding. According to the Ninth Circuit, the plaintiffs' alleged injury in *Krottner* did not rely on a "speculative multi-link chain of inferences," unlike in *Clapper*. As the Ninth Circuit stated in *Krottner*, the threat would have been far less credible 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.

Notably, the Ninth Circuit's decision may make certain Payment Card Industry (PCI) cases 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. Moreover, the court's decision that standing is to be evaluated as of the filing of the complaint may preclude district courts from considering post-filing developments, such as the cancellation of credit cards, when determining standing, although this information would remain relevant for other types of motions.

Another important takeaway is the Ninth Circuit's reliance on the advice Zappos communicated to affected customers in its breach notice. The court noted that "the information taken in the data breach still gave hackers the means to commit fraud or identity theft, as Zappos itself effectively acknowledged by urging affected customers to change their passwords on any other account where they may have used 'the same or a similar password.'" Because the Ninth Circuit arguably "punished" Zappos for

the warnings in its breach notice, companies should re-assess the language in their standard notices to determine whether similar language could be later construed as evidence in favor of a class plaintiff.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston

Partner – Washington, D.C.
Phone: +1.202.624.2775
Email: jposton@crowell.com

Nathanial J. Wood

Partner – Los Angeles
Phone: +1.213.443.5553
Email: nwood@crowell.com

Brandon C. Ge

Counsel – Washington, D.C.
Phone: +1.202.624.2531
Email: bge@crowell.com