Smart in your world®
Arent Fox

Alerts

District Court Finds Lack of Standing for Cyber Data Breach Victims

June 15, 2015
The United States District Court in Nevada issued an Order on June 1, 2015 dismissing the complaint filed by alleged victims of a data security breach suffered by Amazon.com d/b/a Zappos.com (Zappos) on the ground that the victims lacked standing to sue because they could not identify any specific harm that they had sustained as a result of the data breach three-and-a-half years after the data breach had occurred.

In *In re Zappos.com, Inc., Customer Data Security Beach Litigation*, No. 12 CV 00325, 2015 WL 3466943 (D. Nev. Jun. 1, 2015), a multidistrict litigation case, the plaintiffs, a total of twelve people, purported to represent the class of approximately 24 million victims whose personal information had been obtained by hackers who had gained access to Zappos servers. On January 15, 2012, Zappos servers located in Kentucky and Nevada were targeted by one or more hackers. The hackers breached the servers and stole the personal identifying information of approximately 24 million Zappos customers. Zappos notified the affected customers and several lawsuits were filed by consumers against Zappos seeking damages. Following unsuccessful attempts at mediation, Zappos moved to dismiss the complaints on the grounds that the plaintiffs lacked standing to bring their suits.

Zappos's motion to dismiss contended that the plaintiffs lacked standing because they had not alleged any actual damages or specific harm arising from the data breach. Plaintiffs countered that (1) they had standing because the breach had created an increased risk that they would become victims of identity theft or other fraudulent activities because their personal information had been jeopardized; and (2) the breach had devalued their personal information.In addition, three of the twelve plaintiffs who had voluntarily purchased credit monitoring services argued that the cost thereof satisfied the injury-in-fact standard and justified their standing to sue. *In re Zappos.com,* 2015 WL 3466943, at *1-2.

In granting Zappos's motion to dismiss, the court examined recent US Supreme Court opinions on the subject and applied a recent slew of cases analyzing standing in identity theft cases. First, the court dismissed plaintiffs' argument that the breach had diminished the value of their data because plaintiffs failed to explain how the breach rendered their personal information less valuable: "Even assuming that plaintiffs' data has value on the black market, Plaintiffs do not allege any facts explaining how their personal information because less valuable as a result of the breach or that they attempted to sell their information and were rebuffed because of a lower price-point attributable to the security breach. *Id*. at 3 (citations omitted).

Next, in addressing whether the plaintiffs had adequately alleged facts that supported the contention that they faced an increased threat of future harm, the court addressed a purported conflict between the Ninth Circuit and the majority of other federal circuit courts that have addressed the issue following the Supreme Court's decision in *Clapper v. Amnesty International*, ___ US ___, 133 S.Ct. 1138 (2013).

In *Clapper*, a case concerning the potential surveillance of communications between lawyers and certain clients living abroad, the US Supreme Court rejected the Second Circuit's reasoning that standing could be based on "an objectively reasonable likelihood" that the plaintiffs' communications with their foreign contacts would be intercepted in the future. *Clapper*, 133 S.Ct. at 1147. The Supreme Court found that the plaintiffs lacked standing because the alleged harm was speculative and not "certainly impending," *Id*. at 1148.

As the *Zappos* Court noted, the majority of post-*Clapper* cases to deal with data breach have interpreted *Clapper* to mean that the increased risk of identity theft following a breach is insufficient to satisfy the injury-in-fact requirement for in federal court. See *Zappos*, 2015 WL 3466943, at *4-5 (collecting cases). In contrast, the *Zappos* Court recognized that courts in the Ninth Circuit, following *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), have held the opposite. Krottner held 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 [of the US Constitution].'*Zappos*, 2015 WL 3466943, at *5 (quoting *Krottner*, 628 F.3d at 1143). But where other courts have viewed *Clapper* as directly overruling *Krottner* (see, e.g., *In re SAIC*, 45 F. Supp. 3d 14, 28 (D. DC. 2014)), the *Zappos* Court joined two other recent California federal district courts in concluding that the two decisions – *Clapper* and *Krottner* – could be harmonized. See *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,* 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014); *In re Adobe Sys., Inc. Privacy Litig.,* No. 13 CV 05226, 2014 WL 4379916, at *8 (N.D. Cal. Sep. 4, 2014))

Zappos recognized that the test for standing under *Krottner* requires: (1) the plaintiff to face a "credible threat of harm;" and (2) the harm must be "both real and immediate." *Zappos*, 2015 WL 3466943, at *6 (quoting *Krottner*, 628 F.3d at 1143). Zappos interpreted these requirements to be essentially the same as those set forth by the US Supreme Court in *Clapper. Zappos,* 2015 WL 3466943, at *6. Thus, *Zappos* followed *Krottner's* test for standing.

Zappos held that the plaintiffs' alleged harm was simply too speculative to support their claim of standing. The court held that the

Related People

James M. Westerlind

Related Practices

Insurance & Reinsurance

passage of three-and-a-half years since the initial data breach coupled with the absence of any documented harm to the plaintiffs flowing therefrom meant that the alleged harm did not satisfy the standing requirement: “The more time that passes without the alleged future harm actually occurring undermines any argument that the threat of harm is immediate, impending, or otherwise substantial.” *Id*. at *8 (citation omitted).

The court also distinguished the *Zappos* plaintiffs’ from those *in In re Adobe Sys., Inc. Privacy Litig*., No. 13-cv-05226-LHK, 2014 WL 4379916 (N.D. Cal. Sep. 4, 2014), and *In re Sony Gaming Networks & Consumer Data Sec. Breach Litig*., 996 F. Supp. 2d 942 (S.D. Cal. 2014), where the courts held that the standing requirements were satisfied. In *Adobe*, stolen credit card information began to surface within a year of the breach, and hackers used the information to discover vulnerabilities in other *Adobe* products. In *Sony*, the plaintiffs actually experienced unauthorized charges to their credit cards. In *Zappos*, by contrast, plaintiffs did not experience any actual harm, and there was no documentation that their personal data had surfaced even though more than three years had passed.

Finally, the court rejected plaintiffs’ argument that their purchasing of credit monitoring services constituted an injury-in-fact. The plaintiffs could not “manufacture standing merely by inflicting harm on themselves based on their fears of a hypothetical future harm that is not certainly impending.” *Zappos*, 2015 WL 3466943, at *10 (quoting *Clapper*, 133 S.Ct. at 1151). In order for “costs incurred” in an effort to mitigate the risk of future harm to qualify as an injury-in-fact, the future harm must be imminent. Id. Thus, even though the court found the threat of harm credible, the threat’s lack of imminence because of the passage of time without any identifiable harm caused by another meant that the plaintiffs lacked standing.

Zappos is another of a recent line of decisions that has required there to be actual harm, or the immediate threat of such harm, for a victim of a data security breach to sue. Arent Fox is well positioned to assist its clients in understanding how the nuances of unique factual situations affect the issue of standing in the context of data breaches.

Please contact James Westerlind or Andrew Dykens from Arent Fox LLP to discuss this decision or these issues further.