**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

# The Great Data Breach Standing Circuit Split

By **Amanda Lawrence, Antonio Reynolds, Michael Rome and Daniel Paluch** (January 25, 2019, 3:29 PM EST)

Amanda Lawrence

Antonio Reynolds

Michael Rome

Data breaches are back in the news in a big way. Over the past several weeks alone, prominent hotel chains, online platforms and retailers announced significant data breaches. Unsurprisingly, in the aftermath of these disclosures, consumers filed class actions alleging that the data breaches resulted from a failure to maintain reasonable security procedures.

The prompt filing of these lawsuits after disclosure of the breaches highlights a question litigants and courts have been grappling with for years: Does a data breach harm any particular consumer? The answer to this question is critical because in the absence of a specific statute providing for a data breach-related cause of action, a plaintiff ordinarily must prove that he or she has suffered harm in order to have standing to sue.

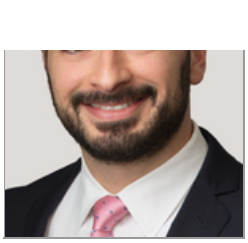
Data breach cases present particularly thorny standing issues. That is because the occurrence of a data breach in and of itself does not necessarily cause a consumer to suffer any specific harm beyond the exposure of the compromised data. And it is not always the case that the exposure of data alone causes the consumer to suffer any cognizable, redressable or concrete harm.

The question of whether (and how) a data breach harms a consumer may be answered by the U.S. Supreme Court this term. In Frank v. Gaos, the Supreme Court requested additional briefing on whether the consumers involved in a disputed privacy class action settlement had standing to sue based on a large online search provider's allegedly unauthorized sharing of search queries with websites the consumers visited.[1] This request for additional briefing was notable in light of the fact that the issue originally before the Supreme Court was not primarily focused on standing issues. While Frank does not involve a fact pattern typical of most data breach cases, it does involve the intersection of standing and purportedly unauthorized disclosure of data. Thus, the Supreme Court may use this case as an opportunity to put this issue to rest once and for all or issue a ruling that provides further guidance for data breach cases.

Given the possibility that the Supreme Court may weigh in on this issue in the near term, it is important to understand how the federal circuits have ruled with respect to standing issues in data breach cases. Indeed, federal appeals courts have split on the issue of whether a data breach — in and of itself, and without evidence of subsequent misuse of the data — is sufficient to confer standing on a consumer.

As set forth below, in the Ninth, Sixth, Seventh and D.C. circuits, a data breach standing alone may be sufficient to confer standing. On the other hand, the Second, Fourth and Eighth circuits require proof of more concrete harm. Moreover, a review of the cases discussed below makes clear that the standing analysis is contingent, in part, on the nature of the breach and the

standing analysis is contingent, in part, on the nature of the breach and the sensitivity of the information accessed or stolen.



Daniel Paluch

**Increased Risk of Future Harm Standard: The Ninth, Sixth, Seventh and D.C. Circuit Holdings**

Recently, in In re Zappos,[2] the U.S. Court of Appeals for the Ninth Circuit adopted a pro-consumer position on standing in data breach cases. In so doing, it joined the Sixth, Seventh and D.C. circuits, all of which have held that the increased risk of future harm from data breaches may be sufficient confer standing to sue even in the absence of specific subsequent harm to the consumer.[3]

Zappos was a putative class action against a large online shoe retailer filed in the wake of a network breach that occurred in or about January 2011. The hackers who perpetrated the breach stole personal account information for over 24 million of the retailer's customers. The stolen data included customer names, email addresses, billing and shipping addresses, phone numbers, credit card numbers, and hashed passcodes. The plaintiff-consumers fell into two categories: (1) those who alleged that they suffered financial losses because their stolen data already had been used to commit identity theft or fraud, and (2) those who did not allege any financial loss as a result of the breach.

The defendant moved to dismiss claims by the latter group of plaintiffs (i.e., those who did not allege the breach caused them any specific financial loss) on standing grounds, arguing that they failed to allege actual harm. While the district court granted the motion,[4] the the Ninth Circuit reversed, finding that these plaintiffs had standing to sue regardless of whether they alleged financial harm. The Ninth Circuit focused on the type of data stolen — including names, addresses and credit card information — and the sensitivity of the data compromised during the breach when it concluded that the data breach created a substantial risk of future identity fraud or theft sufficient to confer standing.[5]

This holding by the Ninth Circuit, while not unique, is noteworthy for two reasons. First, it represents a further split from stricter standing requirements applied by other circuit courts. Second, it acknowledges that data breaches and data theft may deserve redress even if they pose a risk of injury that is markedly different from the types of cases that typically find their way into federal court.

Specifically, the Zappos court noted that "the plaintiffs who alleged that the hackers had already commandeered their accounts or identities using information taken from [the defendant] specifically alleged that they suffered financial losses" because of the data breach, "which is why the district court held that they had standing."[6] The court further noted that other plaintiffs who had not yet suffered financial harm claimed that their email accounts were hacked and used to send advertisements to people in their address books. Given this information, and the nature of the stolen data, the Ninth Circuit reasoned that it was highly likely that the plaintiffs who had not yet suffered financial harm would suffer from identity theft or identity fraud as a result of the breach, even if that theft or fraud would not happen for several years.

As noted above, this "increased risk of future harm" standard also has been adopted in the Sixth, Seventh, and D.C. circuits. However, as discussed below, the Second, Fourth and Eighth circuits reject this approach to standing in data breach cases.

**Increased Risk of Future Harm Is Insufficient: The Second, Fourth and Eighth Circuit Holdings**

In contrast to the Ninth Circuit, the Second, Fourth and Eighth circuits, have held that an increased risk of future harm is not sufficient to confer standing in a data breach case. Instead, in these circuits, some sort of concrete financial harm is typically required.

For example, in In re SuperValu Inc., the U.S. Court of Appeals for the Eighth Circuit found that only one plaintiff whose credit card information was stolen in a 2014 hack of a retail grocery store chain had standing to sue.[7] In that case, the stolen information included names, credit or debit card account numbers, expiration dates, PINs, and CVV codes but did not include any personally identifying information such as Social Security numbers, birthdates, or driver's license numbers.

The Eighth Circuit permitted the one plaintiff's case to go forward because he suffered a present injury in the form of a fraudulent charge on the credit card he used to make a purchase at one of the defendants' stores affected by the data breach in question.[8] However, the Eighth Circuit concluded that his co-plaintiffs, who only alleged a future injury in the form of a fear that their stolen information could be used to commit identity theft, had not plausibly plead an injury sufficient to confer standing.[9] The circuit court focused on the fact that the only factual support in the complaint for the allegation that data breaches facilitate identify theft was a 2007 U.S. Government Accountability Office report. In reviewing that report, the court noted that the report found that most data breaches have not resulted in detected incidents of identity theft. Thus, the court concluded that allegations of future injury were insufficient to confer standing under the circumstances.[10]

The U.S. Court of Appeals for the Fourth Circuit reached a similar conclusion in Beck v. McDonald.[11] Beck was a putative class action filed by veterans who received medical treatment and health care at a Veterans Affairs medical center in South Carolina. This consolidated case arose from reports that boxes of medical records and a laptop containing unencrypted personal information of several thousand patients were stolen. The putative class representatives sued on behalf of a class of plaintiffs who allegedly were injured as a result of the data theft because they faced the threat of future substantial harm from identity theft and other misuse of their personal information.

The court, however, held that the plaintiffs in Beck did not have standing to sue because their alleged harm required the court to engage in an "attenuated chain of possibilities," including making assumptions that the thief targeted the stolen laptop for the information it contained, and would then successfully use the personal information of the named plaintiffs to steal their identities.[12] Nor were allegations that the plaintiffs would have to incur mitigation expenses in the form of financial and credit monitoring sufficient to confer standing, because such expenses do not qualify as "actual injuries" where the underlying harm is not imminent.[13]

Given the speculative nature of the plaintiffs' harm, the court held that the plaintiffs had not suffered an injury-in-fact that could confer standing. Notably, in holding that the plaintiffs in Beck did not have standing to sue, the Fourth Circuit explicitly distinguished this case from cases in the Sixth, Seventh and Ninth circuits on the basis that (1) there was no allegation that the data thief intentionally targeted the personal information compromised in the breach and (2) no named plaintiff in Beck alleged misuse or access of the stolen information.[14]

**Conclusion**

The differing standards for standing in data breach cases have significant consequences for data breach litigation. While plaintiffs in the Sixth, Seventh, Ninth and D.C. circuits may have an easier time surviving the pleadings stage depending on the nature of the allegations and the type of data stolen, plaintiffs in the Second, Fourth and Eighth Circuit and elsewhere will continue to fight an uphill battle to establish standing to sue.

The Ninth Circuit's opinion in Zappos deepened an already significant circuit split on this issue. Given this significant split, it is perhaps unsurprising that the Supreme Court signaled — by requesting supplemental briefing on standing in Frank v. Gaos — that it may weigh in on this issue soon. In the interim, class action plaintiffs attorneys are likely to focus on the Ninth Circuit and like-minded sister courts when deciding where to file data breach class actions.

---

*Amanda R. Lawrence and Antonio Reynolds are partners and Michael A. Rome is counsel at Buckley LLP.*

*Daniel Paluch, formerly with Buckley, is now an associate at Miller Barondess LLP.*

[1] Frank v. Gaos, Case No. 17-961.

[2] In re Zappos , 888 F.3d 1020 (9th Cir. 2018)

[3] See Galaria v. Nationwide Mut. Ins. Co. , 663 Fed. App'x. 384 (6th Cir. 2016); Remijas v. Neiman Marcus Group, LLC , 794 F.3d 688 (7th Cir. 2015); Attias v. CareFirst, Inc. , 865 F.3d 620 (D.C. Cir. 2017).

[4] Zappos, 888 F.3d at 1024.

[5] Id. at 1027–28.

[6] Id. at 1027.

[7] In re SuperValu, Inc. , 870 F.3d 763 (8th Cir. 2017)

[8] Id. at 774.

[9] Id. at 771–72.

[10] Id.

[11] Beck v. McDonald , 848 F.3d 262 (4th Cir. 2017)

[12] Id. at 275.

[13] Id. at 276–77.

[14] Id. at 274–75.