Risk of future identity theft may be sufficient to confer standing in data breach litigation

James J. Giszczak, Christopher G. Dean | Tuesday, March 6, 2018

Over the last decade, something of a circuit split has developed among courts addressing data breach litigation. Until recently, most courts held that a plaintiff who only alleged that his or her information had been accessed by a hacker, but could not allege a concrete injury – such as identity theft – lacked standing to sue for the data breach. These courts tended to view potential damages from the mere disclosure of personal information as speculative and conjectural in that they would flow, if at all, from an injury that had yet to occur. However, in 2017, data breach plaintiffs had more success in persuading federal courts that even in the absence of actual identity theft, they had pled a constitutional injury sufficient to confer Article III standing. These cases may indicate an easing of the burden for plaintiffs to withstand motions to dismiss where personal information is accessed by a hacker, but not yet used.

Attias v. Carefirst, Inc.

In *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017), for example, medical insureds brought a putative class action against a health insurer after certain personal information was stolen during a 2015 data breach. The district court dismissed the complaint for lack of standing, but the U.S. Court of Appeals for the District of Columbia Circuit reversed, concluding that the plaintiffs "plausibly alleged a risk of future injury that is substantial enough to create Article III standing." According to the court, "Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury." The court emphasized that the remaining question was whether the complaint "plausibly alleges that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence in the data breach." Carefirst has petitioned the U.S. Supreme Court for review.

Yahoo! Inc. Customer Data Security Breach Litigation

Similarly, in *Yahoo! Inc. Customer Data Security Breach Litigation*, No. 16-MD-02752-LHK, 2017 WL 3727318 (N.D. Cal., Aug. 30, 2017), the U.S. District Court for the Northern District of California found that Yahoo had to face nationwide litigation brought on behalf of more than one billion users who claimed that their personal information was compromised following three major data breaches between 2013 and 2016. The court held, "All plaintiffs ha[d] alleged a risk of future identity theft, in addition to loss of value of their personal identification information" and "a credible threat of real and immediate harm." Accordingly, the court denied Yahoo's motion to dismiss for lack of Article III standing.

Kuhns v. Scottrade, Inc.

The U.S. Court of Appeals for the Eighth Circuit also dealt with data breach cases suggesting that de minimus harm may be sufficient to convey standing. In *Kuhns v. Scottrade, Inc.*, 868 F.3d 711 (8th Cir. 2017), for instance, the court found that contractual obligations to protect a consumer's personally identifiable information can satisfy Article III standing requirements.

In re: SuperValu, Inc.

Similarly, in *In re: SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017), the court found that standing could exist for a plaintiff based on only one instance of a fraudulent charge on a credit card, even where the plaintiff did not allege that the charge was unreimbursed. The court did note, however, that standing under Article III presents only a "threshold injury," and that the damages claim could fail to meet the "higher hurdles" of Rules 8(a) and 12(b)(6).

The recent shift in case law has significant implications for how companies should prepare for a data breach and possible class action litigation. For questions or information on data privacy and cybersecurity litigation, please contact one of the attorneys below.

James J. Giszczak

Christopher G. Dean