Data Breach Standing: Recent Decisions Show Growing Circuit Court Split

Related Practices

Directors, Officers, Professional, and Corporate Liability Coverage

By Peabody & Arnold on August 31, 2017

It is often said that experiencing a data breach is not a question of if, but when. As we have seen in recent years, data breach litigation is just as inevitable. As companies struggle to deal with data breaches, courts have also struggled to deal with the issue of standing in data breach litigation.

A key battle in data breach litigation is whether plaintiffs have alleged a sufficient injury-in-fact to support standing under Article III of the Constitution. Plaintiffs typically allege that the increased "risk of future harm," such as future fraudulent charges or identify theft, satisfy the injury-in-fact requirement. The United States Supreme Court has held that to establish injury-in-fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). With respect to the "risk of future harm," the Supreme Court has stated that the "threatened injury must be certainly impending to constitute injury-in-fact" and plaintiffs must show a "substantial risk that the harm will occur." *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013).

A series of recent rulings shows a significant circuit split as to whether an increased risk of future harm is sufficient to support Article III standing. Most recently, in August of 2017, the D.C. Circuit held that the plaintiffs "plausibly alleged a risk of future injury that is substantial enough to create Article III standing." *Attias v. CareFirst, Inc.*, 2017 WL 3254941 (D.C. Cir. Aug. 1, 2017). The D.C. Circuit concluded that the combination of information that the plaintiffs had alleged had been stolen, which included social security and credit card information, "make up, at the very least, a plausible allegation that plaintiffs face a substantial risk of identify fraud." The Court further noted that it is "much less speculative – at the very least, it is plausible – to infer that [the hacker] has both the intent and ability to use that data for ill." In addition to the D.C. Circuit, the Sixth, Seventh, and Eleventh Circuits have held that an increased risk of future harm is sufficient to support standing. *See Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012); *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. Appx. 384 (6th Cir. 2016). On the other hand, the Second and Fourth Circuits have held that allegations of nothing more than an increased risk of future injury do not support standing. *Whalen v. Michaels Stores, Inc.*, 2017 WL 1556116 (2d Cir. May 2, 2017); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017).

Given the circuit split and increasing frequency of data breach litigation, it is likely the Supreme Court will need to address this issue which has important implications for corporate liability for data breaches.

