Client Alert: Supreme Court Cert Denial Leaves Confusion in Determining Standing in Class Action Data Breach Cases

Related Attorneys

Eric W. Richardson

Jacob D. Mahle

Brent D. Craft

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 3.28.2018

By: Eric W. Richardson, Jacob D. Mahle, Brent D. Craft and Timothy C. Dougherty

The United States Supreme Court denied a petition for a writ of certiorari last month in *CareFirst, Inc. v. Attias,* No. 17-641, 2017 WL 5041488 (U.S. Oct. 30, 2017), permitting a data breach class action to proceed against a medical insurer. In doing so, the Court passed on an opportunity to resolve the confusion among lower courts in determining Article III federal standing for such cases or, in other words, when a plaintiff can bring suit as a result of a data breach.

The Supreme Court addressed standing in a non-data breach context in the case of *Clapper v. Amnesty Int'l USA,* 568 U.S. 398 (2013). In that case, the Supreme Court reiterated that, in order for a plaintiff to have standing to invoke the jurisdiction of federal courts under Article III of the United States Constitution, a plaintiff must allege an injury that is actual or imminent. *Id.* at 402. Although the mere possibility of injury does not establish standing, a "substantial risk" of injury can be sufficient to create Article III standing. *Id*. at 409, 414 n. 5. In *Clapper*, the court held that the named plaintiffs lacked standing to challenge a provision of the Foreign Intelligence Surveillance Act (FISA) which permitted electronic surveillance of individuals who are not "United States persons" and who are reasonably believed to be outside the United States. *Id*. at 403-404, 417-18. Although the named plaintiffs—consisting of human rights groups, lawyers, media organizations and others—claimed that their communications with foreign contacts were likely to be intercepted in this program, the Court held that, because they could not demonstrate that their communications had, in fact, been intercepted, they could not demonstrate injury and therefore lacked standing to maintain the suit. *Id*. at 410-11. *Clapper* also held that voluntarily assuming mitigation costs were not sufficient—on their own—to establish injury. *Id*. at 1151.

Following *Clapper*, a circuit split has persisted regarding the issue of standing in the context of data breach class actions. On one side, a number of circuit courts have held that—even in the absence of proof

that one's personal information actually has been misused—the mere fact that the information was accessed and/or that the victims of the breach incurred costs as a result of the unauthorized access (*e.g.*, credit monitoring) posed a sufficient risk of injury to confer standing. *See, e.g., Attias v. CareFirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017) (concluding that "simply by virtue of the hack and the nature of the data" alleged to be taken, substantial risk of injury to plaintiffs existed, even though no proof of actual misuse had yet been shown); *Galaria v. Nationwide Ins. Co.*, 663 Fed. App'x 384, 386, 391 (6th Cir. 2016) (holding that standing existed where Social Security numbers were accessed and credit monitoring costs to mitigate the potential identity theft were incurred); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016) (holding that standing existed where credit card information was stolen and plaintiffs incurred charges to mitigate potential effects of breach); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) (pre-*Clapper* decision affirming standing where there was merely an "increas[ed] risk of future harm"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (pre-*Clapper* decision holding that a "credible threat" of identity theft was sufficient to show injury after theft of laptop with personal information).

Other circuit courts, however, have held that plaintiffs, in order to have standing to sue, must demonstrate that their personal information was not only accessed in a data breach, but was actually misused as a result (*e.g.*, a fraudulent line of credit being taken out in the victim's name). *See, e.g., Beck v. McDonald,* 848 F.3d 262, 274-76 (4th Cir. 2017) (rejecting argument that mitigation costs constituted "injury," and holding that injury can be "reasonably likely" to occur based on theft of personal information but still not be sufficiently "imminent" to provide a plaintiff standing to sue); *In re SuperValu, Inc.*, 870 F.3d 763, 769-72 (8th Cir. 2017) (holding that the existence of a data breach—by itself—was insufficient to establish standing, even though credit card information was accessed and one plaintiff faced a fraudulent charge but did not suffer a loss from it); *Whalen v. Michaels Stores, Inc.*, 689 Fed. App'x 89, 90 (2d Cir. 2017) (rejecting standing where stolen credit card was promptly cancelled after the breach and no other personally identifying information was alleged to be stolen); *Reilly v. Ceridian Corp.,* 664 F.3d 38, 42-44 (3d Cir. 2011) (pre-*Clapper* decision holding that "hypothetical future injury" is "insufficient to establish standing" where plaintiffs could only speculate as to whether the hacker obtained, understood, and intended to misuse individuals' personal information).

Whether or not *CareFirst* was the most appropriate vehicle for the Supreme Court to weigh in on this issue, the Court's decision to deny review ensures that lower courts must continue to proceed with a lack of needed clarity in applying *Clapper* to data breach cases. For additional information regarding the ongoing circuit split on the standing issue, please contact your Vorys attorney and consult the 2017 Vorys Whitepaper on the topic, *Consumer Class Actions Arising from Data Breaches Present a Battleground for Standing to Bring Suit*.