THE NATIONAL LAW JOURNAL
FEBRUARY 13, 2018
Online Feature
An ALM Publication

Supreme Court Asked, Again, to Weigh In on Data Breach Standing as Circuit Split Widens

A Supreme Court ruling in a recent case would help clarify the standing issue for the lower courts, consumers and companies that suffer data breaches.

BY CRAIG A. NEWMAN AND JONATHAN HATCH

CareFirst, a large health care company involved in a data breach case, has asked the U.S. Supreme Court to weigh in on whether victims can establish Article III standing to sue for the risk of future identity theft. The issue has split the federal appellate courts, with the U.S. Court of Appeals for the District of Columbia recently holding in *CareFirst v. Attias* that consumers could successfully plead such a claim.

Earlier this year, the high court declined to review another data breach case, *Robins v. Spokeo,* after the Ninth Circuit found that a plaintiff might be able to plead future injury related to false background information published by a website as an intangible injury sufficient to satisfy the "concrete injury" requirement for standing.

At issue in the CareFirst case is whether consumers can assert claims for the risk of harm due to the potential misuse of information obtained through a data breach. The district court dismissed complaints related to a 2015 breach at the large health care company, finding that increased risk of identity theft was too speculative to establish standing. The D.C. Circuit reversed, holding that plaintiffs demonstrated a substantial risk of future harm "by virtue of the hack and the nature of the data."

The Sixth, Seventh and Ninth circuits have ruled similarly, in *Galaria v. Nationwide Mutual Insurance,*

Lewert v. P.F. Chang's China Bistro and *Krottner v. Starbucks*, respectively. The Third, Fourth and Eighth circuits have disagreed, finding the "enhanced risk of future identity theft to be too speculative."

While the specific allegations differ in each case, the decisions have led to a split between circuits, presenting a significant challenge attempting to reconcile the existing case law.

Two recent district court decisions from New York are illustrative. In *Fero v. Excellus Health Plan*, U.S. District Judge Elizabeth A. Wolford of the Western District of New York navigated conflicting case law by relying, in part, on the nature of the information disclosed in a breach. Excellus, a health care provider, had been the victim of breaches in which hackers had accessed information such as names,

dates of birth, Social Security numbers and prior medical claims. Certain plaintiffs solely alleged injury due to the increased risk of future identity theft. Last month, on a motion for reconsideration, Wolford reversed her prior decision dismissing those claims and found that the Second Circuit's unreported decision in *Whalen v. Michaels Stores* suggested that it, too, would find the risk of future identify theft sufficient to confer standing under certain circumstances.

In *Whalen*, a breach resulted in the disclosure of credit card information, but the plaintiff promptly canceled the card so she was not liable for fraudulent charges. A three-judge panel of the Second Circuit affirmed the dismissal of the claims in a summary order, noting that the plaintiff didn't "plausibly face a threat of future fraud, because her stolen credit card was promptly cancelled … and no other personally identifying information … is alleged to have been stolen." It cited in comparison the Sixth Circuit's decision in *Galaria*, which found standing where a hacker obtained personal data including Social Security numbers.

Wolford found the reference to the *Galaria* indicative of how the Second Circuit would evaluate standing where additional information was disclosed. Unlike information relating to only a subsequently canceled credit card, she found that the data disclosed in the Excellus breach could lead to a variety of future fraudulent conduct, and therefore raised an "imminent risk" of future harm. (*See Fero v. Excellus Health Plan*.)

Last fall, another New York district judge reached a similar conclusion using slightly different reasoning in *Sackin v. Transperfect Global.* The case also involved a breach in which hackers accessed an array of consumer information. U.S. District Judge Lorna G. Schofield of the Southern District of New York noted that this disclosure could lead to a variety of fraudulent acts by the hackers (or third parties who subsequently purchased the information) and read *Whalen* to suggest the Second Circuit would recognize this as an injury-in-fact sufficient to establish standing. Schofield further looked to the probable motivation of the hackers, noting that given the nature of the breach, "the most likely and obvious motivation for the hacking is to use plaintiffs' [information] nefariously or sell it to someone who would." She distinguished cases where the motivation behind the breach was less clear (such as in *Beck*, where a laptop was stolen, but there was no evidence that data on the laptop, rather than the laptop itself, was the target of the theft).

While the *Excellus* and *Sackin* decisions are no guarantee of how the Second Circuit might eventually rule, the cases reflect the lower courts' ongoing struggle to resolve the different precedents. A Supreme Court ruling in *CareFirst* would help clarify the standing issue for the lower courts, consumers and companies that suffer data breaches.

Craig A. Newman *is a litigation partner with Patterson Belknap Webb & Tyler in New York and chairs the firm's data security practice group.* ***Jonathan Hatch*** *is counsel with the firm and practices in antitrust, white-collar defense, government investigations and data security.*