Bloomberg Law®

Privacy and Security Law Report®

Litigation

Supreme Court Rejection of CareFirst Review Prolongs Data Breach Standing Circuit Split

Data Breach Litigation

The U.S. Supreme Court's denial of review in *CareFirst v. Attias* leaves courts without further guidance on applying the ''harm'' standard to the standing requirement in data breach cases, but analysis of the leading cases suggests that at least four general factors have influenced judicial decision-making in this area, the authors write.

BY CRAIG A. NEWMAN AND JONATHAN HATCH

On Feb. 21, the U.S. Supreme Court declined to grant certiorari in *CareFirst, Inc. v. Attias*, No. 17-641, in which the U.S. Court of Appeals for the District of Columbia Circuit held that data breach victims could—at the pleading stage—establish standing to sue under Article III of the U.S. Constitution based solely on the risk of future identity theft. Last month, the Court denied review in a similar data security case from the Ninth Circuit, *Robins v. Spokeo, Inc.*, 867 F.3d 1108 (9th Cir. 2017), which found that, as a matter of pleading, the ''concrete injury'' requirement for standing could potentially be satisfied based on a future injury related to false background information published by a website.

CareFirst had argued, in support of its position, that a circuit split had developed regarding the issue of standing for the risk of future identify theft, with U.S. Courts of Appeals for the Third, Fourth, and Eighth Circuits rejecting standing in such instances, and the U.S. Courts of Appeals for the Sixth, Seventh, Ninth, and D.C. Circuits taking a contrary view. Plaintiffs in *CareFirst* had argued that no such circuit split existed, and the former cases were all distinguishable on their facts.

Now, with the Supreme Court's denial of certiorari in *CareFirst*, lower courts are left without further guidance in applying the ''harm'' standard to the standing requirement in data breach cases. Although the facts underlying each breach case are different, as is the risk of consumer harm or injury, our analysis of the leading cases suggests that at least four general factors have influenced judicial decision-making in this area. Below, we examine the leading cases and discuss the factors that have played an important role in the Courts of Appeals' decisions. We also examine some recent cases from the Second Circuit, which have tried to navigate these competing cases in reaching their own conclusions.

Craig A. Newman is a litigation partner with Patterson Belknap Webb & Tyler LLP in New York and chairs the firm's data security practice group.

Jonathan Hatch is counsel with Patterson Belknap in New York and practices in antitrust, white collar defense, government investigations, and data security.

Standing to Sue for Injuries Related to Data Breaches or False Disclosures These cases turn on the issue of standing—the requirement that, under Article III of the U.S. Constitution, federal courts limit themselves to hearing ''actual cases or controversies.'' As the Supreme Court re-emphasized in its decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), to establish standing, a plaintiff must satisfy three elements: that she ''suffered an injury in fact''; that the injury is ''fairly traceable'' to the defendant's conduct; and that that the injury is ''likely to be redressed by a favorable judicial decision.'' To establish the first element, injury in fact, a plaintiff must show that her injury is ''concrete and

particularized'' and ''actual or imminent, not conjectural or hypothetical.''

Standing to plead claims related to the risk of future identity theft involve the first two elements—whether such an injury is actual or imminent, and whether it is fairly traceable to a breach.

Circuits Finding Standing for Risk of Future Identity Theft The Ninth Circuit first addressed standing in this context in 2010. Its decision in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), concerned the theft of a laptop from a Starbucks location containing the names, addresses, and Social Security numbers of nearly 100,000 employees. After Starbucks informed its employees of the theft (and offered a year's worth of free credit monitoring), three employees brought class action complaints for the data breaches. All three alleged that they had devoted time to monitoring their accounts; one pleaded that his bank had notified him that a third party had attempted to open a new account using his Social Security number, though the bank had detected the activity and prevented any losses.

In a relatively brief opinion, the *Krottner* court found that the plaintiffs had satisfied the injury-in-fact requirement, drawing analogies to environmental, medical monitoring, and toxic exposure cases, where plaintiffs were exposed to an increased risk of harm long before the actual injury manifested. The court concluded that plaintiffs faced a ''threat of real and credible harm'' resulting from the theft of their data.

Several years later, the Seventh Circuit joined the Ninth in a pair of opinions. In *Remijas v. Neiman Marcus Group*, 794 F.3d 688 (7th Cir. 2015), a customer brought claims following a data breach at the luxury department store. After hackers gained entry to its system, Neiman Marcus Group LLC determined that hackers had obtained access to approximately 350,000 credit card numbers—9,200 of which were known to have been subsequently used fraudulently. Neiman Marcus was able to confirm that other sensitive information had not been compromised. It then notified its customers of the breach, and offered one year of free credit monitoring and identity-theft protection to affected customers. Several customers who had suffered fraudulent charges on their cards brought a purported class action to recover for an increased risk of future fraudulent charges and identity theft. The plaintiffs conceded that they had been reimbursed for the existing fraudulent charges, and that they did not yet have any evidence that their identities (as opposed to their credit cards) had been stolen. The Seventh Circuit nonetheless concluded that those plaintiffs had pleaded injury-in-fact due to the ''identifiable costs associated with the process of sorting [fraudulent charges] out,'' and that other class members would be forced to continue to monitor their accounts for future fraud—citing Neiman Marcus's offer to provide free monitoring services as evidence that the risk of future fraud was a realistic concern. The court further concluded that ''the Neiman Marcus customers should not have to wait until hackers commit identify theft or credit-card fraud in order to give the class standing,'' noting that delays would make it all the harder for them to prove that any injuries suffered were fairly traceable to the defendant's conduct. It also brushed aside concerns that similar data breaches at other stores might have led to the fraudulent charges, concluding that was an issue to be addressed in discovery.

A year later, the Seventh Circuit reached a similar conclusion in *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016). *P.F. Chang's* involved a data breach at a limited number of the defendant's restaurants in which credit and debit card information had been stolen. Two patrons of P.F. Chang's brought class action suits related to the breach, though neither had dined at a restaurant known to have been affected. One had subsequently suffered fraudulent charges on his credit card; the other had not, but alleged he had spent additional time monitoring his statements. The Seventh Circuit found the circumstances not to be materially different from the pleaded facts in *Remijas*, noting that whether additional restaurants were affected by the breach was a factual dispute to be sorted out in discovery.

The Sixth Circuit, in an unpublished opinion, also followed the Seventh in *Galaria v. Nationwide Mutual Ins. Co.*, 663 Fed. Appx. 384 (6th Cir. 2016). Nationwide is an insurance and financial services company that, in the context of applications for insurance, had obtained personal information from consumers such as names, occupations, employers, Social Security numbers, and driver's license numbers. Nationwide suffered a data breach in 2012 in which hackers stole 1.1 million consumers' personal information. Two consumers brought purported class action suits, alleging that they would suffer the risk of future fraud. One alleged that three efforts had already been made to open credit cards in his name using the information. The Sixth Circuit had little trouble finding that plaintiffs had successfully pleaded their claims, noting that there was ''no need for speculation [about future harm] where Plaintiffs allege their data has already been stolen and is now in the hands of ill-intentioned criminals,'' as ''a reasonable inference can be drawn that the hackers will use the victims data for . . . fraudulent purposes.''

Finally, the D.C. Circuit, in *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017) became the fourth federal appellate court to find that consumers can establish Article III standing by pleading that a data breach increased the risk of their identities being stolen in the future. In 2015, CareFirst, a large healthcare company, announced a data breach, in which an ''unknown intruder'' accessed multiple computers and a database that contained customer names, addresses, and Social Security numbers. Consumers sued, but the district court dismissed their complaint, finding that increased risk of identity theft was too speculative to establish standing. The DC Circuit reversed, holding that plaintiffs demonstrated a substantial risk of future harm ''by virtue of the hack and the nature of the data.''

Circuits Rejecting Standing for Risk of Future Identity Theft Three other circuits, however, have refused to find that plaintiffs plausibly pleaded standing sufficient to bring claims for the risk of future identity theft. The first was the Third Circuit in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011). The defendant in *Reilly* was a payroll processing firm, which suffered a data breach in which an unknown third party potentially gained access to names, addresses, Social Security numbers, and bank account information.'' Some of the affected consumers brought claims related to the risk of future identity theft, increased costs for future credit monitoring, and emotional distress. The Third Circuit found that this amounted to no more than a ''hypothetical'' future

  PVLR ISSN 1538-3423

injury, as there was no evidence that their data had even been copied, let alone that it would be used for future fraudulent activity.

Several years later, the Fourth Circuit joined the Third in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), which concerned a series of data breaches related to medical and personal information at the Veterans' Administration. The first related to the loss or theft of a laptop containing patient records, while the second related to the loss or theft of four boxes of hard copy pathology reports. Distinguishing *Galaria*, *Remijas*, and *Krottner*, the Fourth Circuit dismissed both cases, finding that there was no evidence any of the information had ever been used to commit fraud, that any of the information had been stolen, or, in the case of the laptop, that the data opposed to the laptop itself would have been the target of any theft. *Beck* also specifically rejected the Seventh Circuit's conclusion that the offer of credit monitoring services by a defendant could establish a likelihood of further harm, as it found such an inference ''would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit.''

Several months later, the Eighth Circuit addressed the theft of credit card information by hackers from a chain of grocery stores in *In re Supervalu, Inc.*, 870 F.3d 763 (8th Cir. 2017). Sixteen customers sued based on the risk of future identity theft. One of these customers was also able to allege that he had already suffered fraudulent charges on his credit card. The Eighth Circuit found the distinction between the fifteen plaintiffs who had not yet suffered charges and the one who had to be ''crucial.'' Relying on a Government Accounting Office report that found that the theft of credit card information (without more) to be unlikely to result in identity theft, the Eighth Circuit found that none of the plaintiffs could plausibly plead a risk of future injury. It did, however, allow the final plaintiff to proceed on claims related to past harm as a result of the data breach. In doing so, the court rejected a claim by plaintiff that the need to engage in additional credit monitoring as the result of a breach could itself provide standing, holding that ''the time [plaintiffs] spent protecting themselves against this speculative threat cannot create an injury.''

Attempts to Reconcile Conflicting Case Law: Cases from the Second Circuit Given these contrasting approaches, other courts outside those circuits have had to navigate a thicket of facts and justifications in reaching their own conclusions. Three decisions from the Second Circuit in New York are instructive. The first, the Second Circuit's unpublished opinion in *Whalen v. Michaels Stores, Inc.*, 689 Fed. Appx. 89 (2d Cir. 2017), looked primarily to the nature of the data stolen. In *Whalen*, a breach resulted in the disclosure of credit card information, but the plaintiff promptly cancelled the card so was not liable for fraudulent charges. The Second Circuit affirmed the dismissal of the claims, noting that 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.

While *Whalen* rejected standing on those facts, the citation to *Galaria* suggested that the Second Circuit might be open to finding that other allegations could plausibly plead standing for the risk of future identity theft, and two district courts have cited *Whalen* for just such a conclusion. In a recent decision in *Fero v. Excellus Health Plan*, No. 6:15-CV-06569 EAW, 2018 BL 18253 (W.D.N.Y. Jan. 19, 2018) the district court also navigated conflicting case law by relying, in part, on the nature of the information disclosed in the breach. Excellus Health Plan Inc., a healthcare 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, the court reversed its prior decision dismissing those claims and found *Whalen* suggested that the Second Circuit would find the risk of future identify theft sufficient to confer standing where information beyond credit card numbers was disclosed. Unlike information relating only a subsequently-cancelled credit card, the court found that the type of data involved in the Excellus breach could lead to a variety of future fraudulent conduct, and therefore raised an ''imminent risk'' of future harm.

The court in *Sackin v. Transperfect Global, Inc.*, No. 17 Civ. 1469 (LGS), 2017 BL 356910 (S.D.N.Y. Oct. 4, 2017), used slightly different reasoning to reach a similar result. *Sackin* also involved a breach in which hackers accessed an array of consumer information. The *Sackin* court, as in *Excellus*, 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. The *Sackin* court further looked to the probable motivation of the hackers, noting that given the nature of the breach, ''[t]he most likely and obvious motivation for the hacking is to use Plaintiffs' [information] nefariously or sell it to someone who would.'' It 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).

Common Threads Although the leading case in any given circuit will ultimately control in that circuit, there are important factual distinctions among all these cases that may have an impact on any motion to dismiss claims for risk of future identity theft following a data breach. Among other issues that courts have focused on in deciding the issue are the following:

- **The type of data disclosed.** Courts pay attention to the nature of the data stolen in determining whether future harm is imminent. Numbers for existing credit cards that can be cancelled are less likely to support injury-in-fact related to future identity theft than Social Security numbers or other personally identifying information that can be used more easily to open additional accounts unknown to the affected consumers or commit identity theft.
- **Evidence of prior consequences from the breach.** In *Krottner*, *Remijas*, and *Galaria*, where plaintiffs pleaded that third parties have attempted to make use of the stolen data—even if unsuccessful—the courts found standing. In cases like *Reilly*, and *Beck*, where no such facts were alleged, the cases denied standing.

■ **Motivations behind the breach.** In cases such as *Galaria* and *CareFirst*, courts have adopted the commonsense view that hackers engage in data breaches for the purpose of stealing information and engaging in identity theft or other forms of fraud, and therefore are willing to find imminent risks where plaintiffs plead deliberate hacking. Where, by contrast, the reason for the initial breach is unclear—such as the loss of the laptop in *Beck*—courts are more reluctant to presume that the mere disclosure of data will inevitably lead to fraud.

■ **Free credit monitoring or other remedial services.** When announcing a data breach, a number of companies have offered free credit monitoring or similar services. The *Beck* court rejected outright any argument that an offer of these services could support an inference that future harm was likely or imminent, and most other courts have not otherwise suggested that the offer of services could create standing—giving affected businesses some flexibility in retaining consumer goodwill following a data breach. This is *not* true, however, in the Seventh Circuit, and companies located or with customers in that circuit should be circumspect about providing free credit monitoring, as it may become a factor in a court's motion to dismiss analysis.

These factors are not hard and fast; each has at least one exception. But until the Supreme Court addresses the standing issue, courts are left with little guidance and will continue to look to the specific facts that underlie each data breach in deciding whether a consumer has suffered the requisite ''injury'' to satisfy the Article III standing requirement.

BY CRAIG A. NEWMAN AND JONATHAN HATCH

To contact the editor responsible for this story: Donald Aplin at daplin@bloomberglaw.com

PVLR ISSN 1538-3423