The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No.1 January 17, 2018

STANDING

A Wake-Up Call: Data Breach Standing Is Getting Easier

By Travis LeBlanc, Boies Schiller Flexner LLP, Jon R. Knight, Boies Schiller Flexner LLP

In 2017, consumers in data breach lawsuits were vastly more successful at persuading federal appellate courts that they had pled a constitutional injury. This is a dramatic reversal in the trajectory of federal jurisprudence on "standing" in data breach cases. The Supreme Court had previously held in Clapper v. Amnesty International USA that "conjectural" or "hypothetical" injuries were not sufficient to establish standing and that any alleged harm must be "certainly impending." In the vast majority of data breach class actions, however, consumer plaintiffs have not suffered any actual or imminent harm that they can reasonably connect to a particular breach. These plaintiffs have traditionally faced an almost Sisyphean task to establish standing in the absence of any financial or tangible harm. Indeed, following the Supreme Court's 2016 holding in Spokeo, Inc. v. Robins that a plaintiff must allege an "injury-in-fact" that is "concrete" and "particularized," many commentators and defense counsel expected that plaintiffs would find it even more challenging to establish Article III standing. But, that has turned out not to be the case.

We now have a full calendar-year-worth of federal appellate decisions considering standing for data breach plaintiffs after Spokeo. Contrary to expectations, the trend appears to lean in favor of the class action consumer plaintiff, with four appellate courts finding standing last year, even when consumers had not suffered any actual monetary damages or been the victims of identity theft. Compare that to the two appellate courts that failed to find standing in similar circumstances. This trend should be a wake-up call to companies that collect personal information from consumers. The current willingness of federal courts to entertain consumer plaintiffs' data breach claims has significant implications for how companies should prepare for a data breach and related class action litigation. Expecting that this trend will continue into 2018, companies that experience a data breach should anticipate increased litigation expenses since it will be more difficult to dispose of claims quickly via a motion to dismiss. Now is also a good time for in-house counsel to review incident response plans before a breach occurs to ensure their response team has the litigation skill set necessary to defend complex class actions and government investigations.

See "Third and Seventh Circuits Shed New Light on Spokeo Standing Analysis" (Feb. 8, 2017).

Spokeo Left Unanswered Questions

Spokeo started the trend. Spokeo operates a website that offers users "information about other individuals, including contact data, marital status, age, occupation, economic health, and wealth level." Thomas Robins sued Spokeo under the Fair Credit Reporting Act (FCRA) claiming the company distributed false information about his education and wealth level. The district court dismissed the case for lack of Article III standing since there was no injury-in-fact and any injuries pled were not traceable to Spokeo's alleged FCRA violations. The Ninth Circuit reversed, finding that there was no requirement to allege actual harm because the plaintiff had alleged a willful violation of statute.

Upon review, the Supreme Court reversed, holding that the plaintiff must allege both an individualized injury and a concrete injury in order to satisfy the Article III standing requirement for an injury-in-fact. But the Court did not provide clear guidance on what constitutes a concrete injury. Instead, it stated that "risk of real harm" could satisfy the concreteness requirement. Notably, Spokeo did not resolve the question how much risk must be present or how to quantify the risk.

See "Spokeo's Impact on Data Breach Cases: The Class Action Floodgates Have Not Been Opened, But the Door Has Not Been Locked" (May 25, 2016).

Courts Are Now Approving Several Standing Theories

Traditionally, consumer plaintiffs have had to allege that the defendant's breach caused them a present tangible or financial harm. Speculative, conjectural, or risk of future injury was not enough. Spokeo, however, was less-than-clear regarding what constituted a concrete injury, and could have been viewed as reinforcing a high bar for showing standing. But many federal courts post-Spokeo (and particularly appellate courts) have found standing for plaintiffs even though the plaintiffs alleged little-to-no pecuniary harm and any future harm was not clearly tied to the defendant's conduct. Indeed, the trend suggests that courts have been more willing to confer standing on plaintiffs' allegations of per se injury.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No.1 January 17, 2018

Standing Based on De Minimis Harm

The Eighth Circuit was busy with data breach cases in 2017. In addition to the opinion in Kuhn v. Scottrade, Inc. where the court found that contractual obligations to protect a consumer's personally identifiable information can satisfy Article III standing requirements, the circuit's In re: Supervalu, Inc. decision found there could be standing for plaintiffs based on only one instance of a fraudulent charge on a credit card, even when the plaintiffs did not allege that the charge was unreimbursed. While the court stopped short of finding that allegations of future injury alone could support standing, it found that one potentially reimbursed fraudulent charge was an actual injury sufficient to confer standing. The court also specifically declined to decide whether "evidence of misuse following a data breach is necessary for a plaintiff to establish standing."

See "Eighth Circuit Sides With Defendants As the Spokeo Standing Battle Continues" (Oct. 5, 2016).

Standing Based on a Clear Violation of Federal Law

Moving east, the Third Circuit found standing for data breach plaintiffs in In Re: Horizon Healthcare Services Inc. Data Breach Litigation where the theft of two laptops containing unencrypted personal information led to a putative class action alleging violations of FCRA. The Third Circuit reinstated a class action because "the unlawful disclosure of legally protected information constituted a clear de facto injury." The court's significant statement is that "a focus on economic loss is misplaced" when addressing standing in the privacy context.

Standing Based on Future Risk of Injury

The following cases most dramatically changed the standing landscape for data breach plaintiffs. The D.C. Circuit heard Attias v. Carefirst, Inc., where a class of insureds brought a putative class action against a health insurer after their personal information was stolen during a 2015 data breach. The district court had dismissed the complaint for lack of standing, but the D.C. Circuit reversed. While the plaintiffs had not alleged actual misuse of their stolen personal information, the D.C. Circuit found that "at the very least, it is plausible to infer that [the thief] has both the intent and the ability to use that data for ill." As the judges wrote: "No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken."

Although technically not in 2017, the Sixth Circuit reached a similar result the previous year in Galaria v. Nationwide Mutual Insurance Co., where the plaintiffs' personal information had been stolen in a network breach. They alleged FCRA violations and brought additional claims based on negligence, invasion of privacy by public disclosure of private facts, and bailment. The Sixth Circuit found that, under Spokeo, it was "unreasonable to expect Plaintiffs to wait for actual misuse." With respect to the risk of future harm, the court wrote: "[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. . . . Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." The court concluded that "[p]laintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation."

Going further west, the Ninth Circuit revisited Spokeo after the Supreme Court's remand in 2016. While Spokeo is not a data breach case, it does shed light on the evolving ways in which courts see injury arising from circumstances involving the misuse of personal information. In Spokeo 2.0, the Ninth Circuit again found standing. The court found a concrete injury existed because of the inaccuracies in the consumer report: "Given the ubiquity and importance of consumer reports in modern life – in employment decisions, in loan applications, in home purchases, and much more – the real-world implications of material inaccuracies in those reports seem patent on their face." Rather than seeing the injury as speculative, the court concluded that "[i]t does not take much imagination to understand how inaccurate reports on such a broad range of material facts about Robins's life could be deemed a real harm." Following the Ninth Circuit's decision, Spokeo recently filed another petition for certiorari on the question of "Whether the injury in fact requirement is satisfied by claimed intangible harm to an interest protected by the underlying statute, even if the plaintiff cannot allege that she suffered either real-world harm or an imminent risk of such harm." The Supreme Court is scheduled to consider this petition during its January 19, 2018 conference. Stay tuned.

The Yahoo! Inc. Customer Data Security Breach Litigation illustrates how these ideas are taking hold at the district court level. In denying a motion to dismiss and finding standing for increased risk of future identity theft, a judge in the Northern

District of California echoed what is now becoming a familiar refrain: "Presumably, the purpose of the hack is, sooner or later, to assume those consumers' identities or to misuse Plaintiffs' [personally identifiable information] in other ways." Accordingly, the court found the plaintiffs had alleged a "concrete and imminent threat of future harm sufficient to establish Article III injury-in-fact."

Not All Cases Found Standing

Of course, there is still a circuit split on the issue of standing for claims of increased risk of future identity theft, mostly due to Spokeo's lack of clarity. For example, in Beck v. McDonald, the Fourth Circuit refused to confer Article III standing based on harm from embarrassment, mental distress, inconvenience, the increased risk of future identity theft and the cost of measures to protect against it after (i) a laptop containing plaintiffs' personal health information was stolen and (ii) four boxes with pathology reports went missing. The Fourth Circuit emphasized that there were no allegations of misuse of the personal information by the thief, and that the increased risk of identity theft was too speculative without at least one such allegation.

The Second Circuit similarly found no standing in Whalen v. Michaels Stores, Inc. Here, the details of the plaintiff's credit card were likely taken in a 2014 data breach. While there were attempted fraudulent charges on her account, she quickly canceled her card and no fraudulent charges were actually incurred. In affirming the dismissal for lack of standing, the Second Circuit noted several distinguishing factors for finding there was no increased risk of identity theft: "she does not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information – such as her birth date or Social Security number – is alleged to have been stolen."

See "When Do Consumers Have Standing to Sue Over Data Breaches?" (May 11, 2016).

Understanding the Trend

The foregoing cases indicate a trend towards permitting putative class actions in data breach cases to proceed to discovery without allegations of actual pecuniary harm. This is likely due to two factors.

1. Bigger and More Frequent Breaches

As in past years, breaches in 2017 continued to get bigger and more frequent – with Equifax and Yahoo! being the most notable last year. These large, international breaches seem to be affecting the balance of equities in a legal environment where victims of the breach have little legal recourse. Judges (and elected officials) may sense a public need for more legal accountability in this arena.

2. Evolving Notions of Harm

Legal notions of privacy harm also seem to be evolving from being seen as an invasion of a civil liberty to a property violation. The recent Supreme Court argument in Carpenter v. United States is one of the latest examples of this evolution. Carpenter involved law enforcement access to historic cell tower location information that is retained by cell phone companies – not a data breach. During oral argument, Justice Gorsuch repeatedly asked counsel for both sides to put the reasonable expectation of privacy argument to the side and to explore whether individuals have a property right in their personal information. He posited, "the property-based approach to privacy also has to be considered, not just the reasonable expectation approach. So, if we put aside the reasonable expectation approach for just a moment, Katz, Miller, Smith, and ask what is the property right here, let's say there is a property right." This property-based approach would have several legal implications. For example, if an individual's personal information is wrongfully obtained by an unauthorized third party, the legal wrong might be viewed as a property conversion with associated economic harm under state law.

The Carpenter case has not been decided by the Court yet. But in 2018, we will not be surprised to see the property-based approach to privacy gain traction in federal courts. If it does, this traction will improve the ability of plaintiffs to allege a concrete harm and survive a motion to dismiss.

The Wake-Up Call: Practical Steps for Companies

As with all analyses, there are caveats. Several of the recent cases where the courts found de facto standing involved federal causes of action that were expressly created by Congress. While federal courts may view a legislative finding of per se harm as sufficient to establish a legally cognizable injury to support standing, such statutory violations would not apply to all data breach cases. Additionally, these are all federal court

cases – not state or international courts where Article III is not applicable. These other forums may be undergoing different trends and should be the subject of further study and analyses. Lastly, these data breach decisions are occurring at the motion to dismiss stage of litigation. We do not yet have much insight into how courts will view the increased risk of future identity theft at the summary judgment stage or at trial. In other words, just because a harm is sufficiently concrete to establish standing does not ipso facto convert it into economic damages.

Nevertheless, we believe that in 2018 it is likely that plaintiffs in data breach cases will increasingly prevail on standing and survive motions to dismiss. If, going forward, it will be harder to quickly dispose of data breach claims as this trend suggests, then companies should prepare themselves in advance for this new reality. What does that mean?

1. Prepare for Increased Litigation Expenses

If data breach claims cannot be knocked out quickly through a motion to dismiss, then there will be significantly increased litigation expenses as defendants will face the demands of fact and expert discovery, lengthy motions practice relating to class action defense, and ultimately trial preparation. As the Equifax breach illustrates, this will consume internal resources and require a significantly greater investment in outside counsel. In less than two months after its market-moving breach was announced, Equifax incurred $87.5 million in expenses relating to the breach litigation and government investigations. That was before any settlements or jury verdicts. In addition to reviewing your litigation budget, now may also be a good time to purchase or review your cyber insurance policy.

2. Revisit Incident Response Plans

Incident response plans should include a litigation team with privacy expertise and class action experience. Your incident response plan should reflect a multi-disciplinary approach that incorporates:

- complex litigation management and experience;
- public relations and strategic communications;
- internal investigations and breach response; and
- the ability to respond quickly to government investigations at the state, national, and international levels.

Time is of the essence when a breach occurs. Companies cannot wait until after a breach to identify their response team (and the outside counsel that will lead it) because litigation (and the news cycle surrounding the breach) move far too quickly. For example, Equifax faced more than 20 different class actions within five days after its breach was announced. In less than 3 months, it was fighting over 240 individual class-action lawsuits, a 50-state class action suit, and 60 government investigations from multiple federal agencies, state attorneys general, and British and Canadian regulators. And then there's Congress, too. If an incident response plan does not already lay out a comprehensive team of outside litigation counsel and consultants with experience in complex class action litigation before any breach occurs, then corporate defendants will find themselves at a disadvantage in responding to the inevitable litigation and investigations.

In this evolving litigation environment, pre-breach compliance work must also be done with an eye towards both compliance and litigation strategy. There is plenty of work to be done before a breach occurs to ensure that potential defendants have implemented best practices and are in compliance with applicable laws. But the pre-breach incident planning must also be done with an understanding of how that work will affect the increasingly inevitable post-breach litigation. For 2018, this means involving outside litigation counsel before a breach occurs so that there is a coordinated approach and litigation counsel are ready, willing, and able to respond on a moment's notice.

See our three-part guide to developing and implementing a successful cyber incident response plan: "From Data Mapping to Evaluation" (Apr. 27, 2016); "Seven Key Components" (May 11, 2016); and "Does Your Plan Work?" (May 25, 2016).

Travis LeBlanc, former Chief of the Federal Communications Commission's Enforcement Bureau, is a partner at Boies Schiller Flexner and represents clients in matters related to cybersecurity, privacy, telecommunications, and the regulation of emerging technologies. Drawing on his broad experience in federal and state government, he helps clients manage their litigation, regulatory risk, and strategic responses to data privacy and security incidents, litigation, and government investigations.

Jon R. Knight (CIPP/US) is an associate at Boies Schiller Flexner. He is a litigator who advises clients on variety of issues including intellectual property, cybersecurity and data privacy.