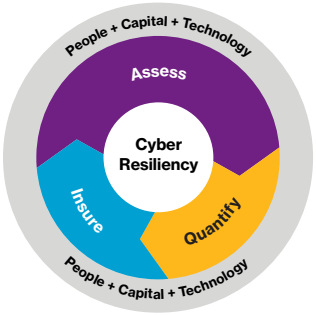


Decode litigation.

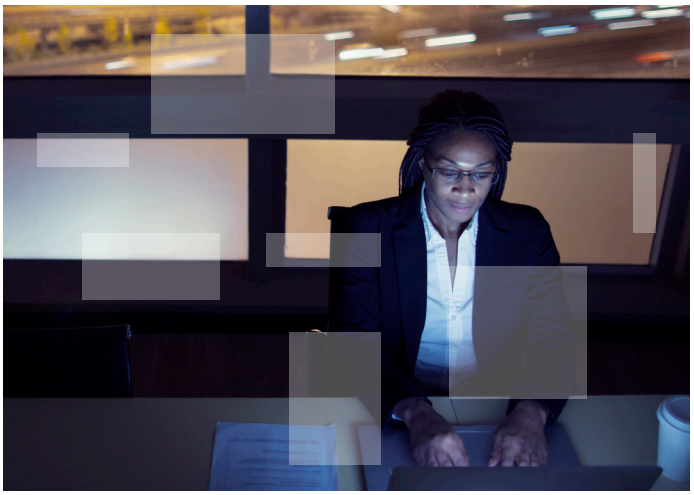
Emerging, high-stakes, cybersecurity litigation and investigations risks are upending the legal landscape

By David Quinn Gacioch, partner, and Natasha Dobrott, summer associate, McDermott Will & Emery LLP

Cybersecurity and data breaches are now part of our daily lives, and are driving rapid changes to the legal landscape. Plaintiffs' lawyers view privacy and cybersecurity as enticing new sources of class action and single-plaintiff litigation work. At the same time, state and federal regulators and law enforcement continue to bring more resources to bear on these areas. In this challenging environment, creators, holders, processors and owners of sensitive data face a myriad of rapidly-changing risks to manage and insure against.

Standing issues in data breach litigation: a primer

In private data breach litigation, the plaintiff usually claims that the defendant employed inadequate safeguards to secure the plaintiff's personal information, which resulted in the breach. Most such plaintiffs are unable to prove that their data has actually been misused by hackers (for identity theft or other purposes), forcing them to rely instead on the risk of future identity theft or similar harm as the basis for their claims. This dependence on the risk of future injury leaves their complaints susceptible to dismissal at the pleading stage for lack of standing – required by the "case or "controversy" requirement of Article III, Section 2, Clause 1 of the United States Constitution for federal court jurisdiction. In order to successfully establish standing, the plaintiff must reasonably plead: (1) an injury-in-fact that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical"; (2) that the injury is "fairly traceable" to the conduct being challenged; and (3) that the injury is likely to be redressed by a favorable judicial decision. Failure to sufficiently allege any one of these three elements is fatal to a complaint.



It is the first prong, injury-in-fact, that poses the greatest challenge to successfully establishing standing in data breach cases. The key question is whether plaintiffs have suffered an injury-in-fact when personal data is exposed to, or taken by, an unauthorized party due to a breach, but not (yet) actually misused to the best of the plaintiff's knowledge. In other words, is the threat of future injury from identity theft or other harmful data misuse, and the time and money spent on precautions to avoid this potential future harm, sufficient to constitute an injury-in-fact? The answer to this question is far from clear and has given rise to disagreement among federal appellate and trial courts across the country. This is not an issue for plaintiffs who can demonstrate that their information has, in fact, been misused to their detriment. However, it poses a problem for plaintiffs who worry about what has happened to their information, but cannot prove that it has actually been sold or misused in a way that harms them.

Courts diverge on *Spokeo*: Are statutory violations sufficient to establish injury-in-fact?

One issue related to establishing injury-in-fact caused by a data breach is a plaintiff's lack of proof of actual damages when a suit is brought based on a defendant's violation of a statute. In May 2016, the U.S. Supreme Court issued its highly-anticipated ruling in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), which addressed Congress' right to confer Article III standing based on a violation of a statute where the plaintiff had not experienced any concrete harm. Spokeo, Inc. is a consumer reporting agency that collects and provides personal information about individuals to a range of users. When Robins realized the profile Spokeo had created about him contained incorrect information, he filed a federal class action complaint against Spokeo under the Fair Credit Reporting Act of 1970 (FCRA). Spokeo asserted that Robins did not have standing because he had not alleged any concrete injury as a result of the incorrect information Spokeo had made available. The District Court dismissed Robins' complaint, determining that he had not sufficiently pled injury-in-fact to satisfy the Article III standing requirements. The U.S. Court of Appeals for the Ninth Circuit reversed the District Court's decision, holding that the statutory cause of action under the FCRA did not require plaintiffs to demonstrate that they had experienced any actual harm and that the "violation of a statutory right" is most often sufficient to establish standing.

The Supreme Court in a 6 to 2 decision held that, in order to satisfy the injury-in-fact-requirement of Article III standing, the injury must be both "concrete" and "particularized." Since the Ninth Circuit's reasoning involved only the "particularized" element, the judgment was vacated and remanded back to the lower court to consider not only whether the injury was particular, but also concrete. While the Court noted that the term "concrete" suggests that the harm is real (not abstract or merely procedural), "concrete" does not necessarily mean that the harm needs to be tangible. "Intangible" harm or even in some cases "risk of harm" can qualify as concrete so as to satisfy the requirement, according to the Court. However, the Constitution's injury-in-fact requirement is not automatically satisfied when a statute gives a person a statutory right and authorizes the person to sue based on an alleged violation of that right. In order to establish an injury, a plaintiff must allege a statutory violation that caused him to suffer some sort of real world harm, not just an abstract or procedural injury.

On remand, the Ninth Circuit found that Robins' injury-in-fact was sufficiently concrete and particularized to confer standing, and it laid out a two-step inquiry for the "concrete" harm requirement:

- Did Congress adopt the statutory provision at issue to protect the individual's concrete interests?
- Did the procedural violations alleged in the case actually harm or pose a threat of real harm to the plaintiff?

Courts continue to diverge in their application of the Supreme Court's broad holding as they attempt to define the concrete harm standard laid out by *Spokeo* – a process not aided by the Supreme Court's recent declination to revisit *Spokeo* after the Ninth Circuit's latest decision in Robins' favor.

Circuit split over standing in data breach cases and future injury

Plaintiffs in data breach litigation continue to be challenged to use the perceived threat of future injury to establish injury-in-fact. The Supreme Court's 2013 decision, *Clapper v. Amnesty International USA,* 133 S. Ct. 1138 (2013) held that, in order for plaintiffs to have Article III standing based on a threat of future injury, they have to demonstrate that the injury is "certainly impending," a difficult burden to meet in data breach cases, which often involve the data of millions of people and a lack of proof that the data has actually been sold or misused. A footnote in the *Clapper* decision denotes what some lower courts have interpreted to be the less strict "substantial risk" test. The Supreme Court case *Susan B. Anthony List v. Driehaus,* 134 S. Ct. 2234 (2014) further acknowledged the substantial risk test as an alternative way of establishing injury in fact, holding that in cases concerning the potential for future injury, the plaintiff must show that the "threatened injury is 'certainly impending' or there is a 'substantial risk'" that harm will occur.

A split has continued to develop among the Federal Courts of Appeals around the country on the issue of risk of future injury in data breach cases. Hybrid situations are particularly gray areas: (1) allegations of present anxiety and worry on plaintiffs' parts, purportedly created by a data breach, and (2) the inconvenience of implementing present measures to protect against future identity theft or data misuse. This circuit split has revealed that in some cases, the anxiety and threat is sufficient, while other courts have held that there needs to be more.

The Second, Fourth and Eighth Circuits have taken the more rigid position, holding that there is no standing where no actual identity theft or fraud occurs as a result of the breach. *See e.g. Whalen v. Michaels Stores, Inc.,* 689 Fed. Appx. 89, 2017 WL 1556116 (2d Cir. May 2, 2017); *Katz v. Pershing, LLC,* 672 F.3d 64 (1st Cir. 2012). The Fourth Circuit in *Beck v. McDonald,* 848 F.3d 262 (4th Cir. 2017), held that, under the precedent set by *Clapper*, the risk of identity theft after information has been taken in an intrusion is too speculative to confer standing. *Beck* involved a laptop containing unencrypted personal information of over seven thousand patients that was likely stolen from a Veterans Administration medical center.

The Eighth Circuit echoed this holding in *In re SuperValu Inc.,* 870 F.3d 763 (8th Cir. 2017), which involved the use of malicious software to obtain access to credit and debit card information of 16 grocery store customers. The stolen card information did not include any personally identifying information, limiting the type of potential future harm that could occur to debit and credit card fraud. The court found that there was no standing because there was no substantial risk that future injury would occur.

In contrast, the Third, Sixth, Seventh, Ninth, Eleventh and D.C. Circuits have taken a more permissive stance on the question, generally holding that the risk or threat of data misuse in data breach cases is sufficient to confer standing. See e.g., I*n re Zappos.com, Inc.,* 888 F.3d 1020 (9th Cir. 2018); *In re: Horizon Healthcare Services Inc. Data Breach Litigation,* 846 F.3d 625 (3rd Cir. 2017); *Remijas v. Neiman Marcus Grp.,* 794 F.3d 688, 693 (7th Cir. 2015); *Resnick v. AvMed, Inc.,* 693 F.3d 1317 (11th Cir. 2012). For example, the Sixth Circuit case, *Galaria v. Nationwide Mutual Insurance Company,* 663 Fed. Appx. 384 (6th Cir. 2016), involved the breach of insurance records containing sensitive personal information of about 1.1 million of Nationwide's customers. The court found that, even though it was not "literally certain" that the data breach would cause harm to customers, there was a sufficiently substantial risk of injury, noting that when hackers specially target personal information, it is a "reasonable inference" that the data will be used for fraudulent purposes.

In February 2018, the Supreme Court declined the opportunity to review the D.C. Circuit's decision in *Carefirst v. Attias,* 865 F.3d 620 (D.C. Cir. 2017) and, through that case, to resolve the circuit split. *Carefirst* involved a health insurer that experienced a cyberattack where the personal information of customers was allegedly stolen. The plaintiffs, a group of Carefirst customers, brought suit against the company, attributing the breach to the company's negligence. The district court dismissed the case for lack of standing, holding that the risk of future injury, which was an increased risk of identity theft, was "too speculative" to satisfy the injury-in-fact requirement.

The case was appealed to the D.C. Circuit, which reversed the district court's decision. The court distinguished this case from *Clapper*, which had involved a provision of the Foreign Intelligence Surveillance Act that permitted surveillance of foreign nationals outside of the United States. The plaintiffs in *Clapper* were United States citizens who brought suit because they asserted that there was an "objectively reasonable likelihood" that their communications with foreign nationals would be intercepted. In that case, however, there were several different steps, involving independent actors, in a chain of events that would have needed to occur in order for the plaintiffs to be harmed. In contrast, the D.C. Circuit found that the likelihood of harm in *Carefirst* was far less attenuated. The court reasoned that information such as birth dates, email addresses and subscriber identification numbers can combine to create a substantial risk of identity theft. In cases like these, the court said that it is entirely plausible that the breaching party has the "intent and ability to use the data for ill."

The case law surrounding the circuit split has revealed that the issue of standing in future injury data breach cases is a highly factually dependent inquiry. Outside of the existing case in each circuit, there are a variety of factors that can sway the court's decision either way. These factors include who stole the data, how it was taken, whether there is any evidence that at least some consumers experienced data misuse, how much time has passed since the breach without evidence of misuse, and the type of data compromised. Even if plaintiffs are able to surmount the injury-in-fact hurdle, they still have to satisfy the other two requirements for standing: causation and damages, which can be difficult, especially for those plaintiffs who suffered no actual out-of-pocket cost.

The Supreme Court's refusal to address the issue in *Attias* and the growing split among the circuits makes it likely that there will be another high court decision at some point in the near future to resolve this issue more definitively. It is also possible that these decisions and any future Supreme Court cases on this issue will also have an impact on class

certification in data breach cases. Until then, litigants in these cases will have to be conscious of the differences among the various circuits when bringing these cases. The D.C., Sixth and Seventh Circuits are likely to become the forums of choice for plaintiffs in data breach cases while the Eighth and Fourth Circuits will be sought out by defendants.

Regulatory roundup

As cybersecurity issues continue to generate both headlines and high-dollar impact, increasingly government agencies are weighing in. Most businesses that deal with sensitive personally identifiable information face the potential for Federal Trade Commission (FTC) scrutiny at the federal level and investigation by one or more attorneys general (AG) at the state level. The recent effective date of the General Data Protection Regulation (GDPR) in Europe is likely to have spillover here in the United States as the FTC and state AGs begin to scrutinize how well GDPR-regulated companies are living up to the commitments made in their new, GDPR-friendly privacy policies. And specialty or sector-specific regulators in the privacy and cybersecurity areas continue to proliferate – including the Securities and Exchange Commission and the Division of Enforcement's nascent Cyber Unit.

One spotlight area is enforcement of the Health Information Portability and Accountability Act (HIPAA) by the U.S. Department of Health and Human Services, Office for Civil Rights (OCR). After several years of relatively minor enforcement activity, OCR entered into record-breaking settlement totals in 2016 and 2017 – doubling prior years' settlement counts and averaging nearly $2 million per settlement, plus a 2- to 3-year corrective action plan featuring intensive OCR supervision of the settling entity. 2016 and 2017 also featured the two largest individual HIPAA settlements in history – at approximately $5.5 million apiece – along with an increased willingness by OCR to impose civil monetary penalties if settlements could not be reached. This is all consistent with public statements that senior OCR officials have made for a few years now, so HIPAA-regulated entities may experience heightened scrutiny for quite some time.

Regular cyber coverage checkups matter

Cyber risks are evolving and multiplying rapidly as liability carriers are increasingly gaining sophistication in these areas. Insureds are well-served to regularly assess the state of their cyber coverage and particularly the evolving interpretations of exclusions or coverage limitations potentially touching on cyber risk.

Contact

David Quinn Gacioch
Partner, McDermott Will & Emery LLP
+1 617 535 4478
dgacioch@mwe.com

Natasha Dobrott
Summer Associate, McDermott Will & Emery LLP
+1 617 535 4000
ndobrott@mwe.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-NA-2018-WTW76711

willistowerswatson.com

Willis Towers Watson