New York Law Journal
Cybersecurity
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 42
MONDAY, MARCH 6, 2017

Do **Mitigation Efforts** Give Plaintiffs A **Right to Sue** in Data Breach Cases?

BY SETH D. ROTHMAN AND DENNIS S. KLEIN

Imagine that your credit card information is stolen in a data breach. Do you have standing to sue the company where the data breach occurred? Most courts would say "no," not unless the hackers misuse your information and you incur fraudulent charges. But if there is a substantial risk that this may happen and you take steps to prevent it, you may be able to recover your mitigation costs.

The Legal Standards

The U.S. Supreme Court recently reviewed the standing requirements in *Spokeo v. Robins*, 136 S. Ct. 1540 (2016). In *Spokeo*, the court confirmed that standing requires an injury-in-fact, i.e., an injury that is "concrete and particularized," and "actual or imminent, not conjectural or hypothetical." Id. at 1548 (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). In the example above—where hackers steal information, but do not use it—plaintiffs have not suffered an actual injury.

For that reason, many data breach plaintiffs seek to establish standing based on an "imminent" injury—i.e., that their information may be misused in the future. To be imminent, however, the injury must be "certainly impending" and not merely possible. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). It is hard to see how plaintiffs could meet this standard in a typical data breach case; it would be a rare plaintiff, indeed, who could show that he or she was literally certain to suffer harm.

Recovery of Mitigation Costs

Clapper may have resolved the question of data breach standing

SETH D. ROTHMAN *and* DENNIS S. KLEIN *are partners at Hughes Hubbard & Reed.*

if the court had not suggested an alternative standard. In a footnote, the court acknowledged that it has found standing based on a "substantial risk" that harm will occur, "which may prompt plaintiffs to reasonably incur costs to mitigate or avoid the harm." Id. at 1150 n.5. Data breach plaintiffs have seized upon this footnote to argue that they have standing to recover their reasonable mitigation costs.

These arguments have met with varying degrees of success. U.S. Courts of Appeals in the Sixth, Seventh and Ninth Circuits have found that, when information is stolen in a data breach, there is a substantial risk that harm will occur—i.e., that the stolen information will be misused. Courts in the Third and Fifth Circuits have been unwilling to conclude that there is a substantial risk of harm without evidence that the stolen information has actually been misused.

At first glance, this appears to be a circuit split. But a close reading of the case law shows that the disparate results have not been driven by different interpretations of *Spokeo* and *Clapper*, but by the particular facts of each case. The existing cases can, in fact, be harmonized: a substantial risk of future harm exists where (1) the circumstances of the data breach suggest that the hackers will misuse the stolen information, or (2) the hackers have misused some of the stolen information. See *Khan v. Children's National Health Systems*, 188 F. Supp. 3d 524, 532 (D. Md. 2016).

Theft of Payment Card Information

In cases where payment card information is stolen, courts have generally found that there is a substantial risk of future harm. As the Seventh Circuit put it, "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Group*, 794 F.3d 688, 693 (7th Cir. 2015). In *Remijas*, the Seventh Circuit found imminent injury where hackers had used malware to collect credit card information from up to 350,000 Neiman Marcus customers. See id. at 696-97; see also *Lewert v. P.F. Chang's China Bistro*, 819 F.3d 963 (7th Cir. 2016) (finding imminent injury where hackers stole credit and debit card numbers from 33 restaurants).

In these types of cases, timing is an issue. If significant time elapses without any harm occurring, the injury is no longer imminent. For example, a court has found that plaintiffs lacked standing where there had been only one unauthorized charge in the 15 months following the breach. *In re SuperValu*, No. 14-MD-2586, 2016 WL 81792, at *5 (D. Minn. Jan. 7, 2016).

Theft of Personally Identifiable Information

In data breach cases where personally identifiable information is stolen, courts have looked more closely at the purpose of the underlying attack. For example, where hackers accessed insurance company records containing the "names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers" of 1.1 million customers, the Sixth Circuit found there was a substantial risk of future identity theft. *Galaria v. Nationwide Mutual Insurance Company*, Nos. 15-3386, 15-3387, 2016 WL 4728027, at *1-*5 (6th Cir. Sept. 12, 2016). The court reasoned that, "[w]here 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." Id. at *3.

If there is a **substantial risk that harm will occur,** plaintiffs may be able to recover the costs incurred to mitigate or avoid that harm.

In contrast, a court found no imminent injury where hackers obtained hospital patient records through an email phishing scheme. The scheme

was designed to gain access to the email accounts of hospital employees, rather than the hospital's "electronic medical records system or some other centralized database of personal data" and "there [was] no indication that the patients' personal data was actually viewed, accessed, or copied." *Khan*, 188 F. Supp. 3d at 532; see also *Reilly v. Ceridian*, 664 F.3d 38 (3d Cir. 2011) (finding plaintiffs lacked standing where it was unknown whether the hacker accessed the plaintiffs' personal data or would have understood it if he did).

When laptop computers are stolen, it may not be clear if the thieves were after the laptops, the personal information contained on the laptops, or both. In such cases, courts have therefore required evidence that the stolen data was actually misused. For example, in a case where thieves stole two laptops containing the unencrypted health information of 1.2 million customers, the court found that plaintiffs faced imminent harm based on allegations that there had been fraudulent activity with respect to two of the plaintiffs. See *Resnick v. AvMed*, 693 F.3d 1317, 1322-24 (11th Cir. 2012); see also *Krottner v. Starbucks*, 628 F.3d 1139 (9th Cir. 2010) (holding plaintiffs suffered an injury-in-fact when thieves stole a laptop containing the unencrypted personal records of 97,000 Starbucks employees and fraudulently set up a bank account in one plaintiff's name).

In another case, thieves broke into a car and stole a GPS, stereo, and computer backup tapes containing "a variety of medical information." *In re Science Applications International (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 20 (D.D.C. 2014). Since it was unknown whether the backup tapes had been "uploaded onto [the thief's] computer and fully deciphered," or were "lying in a landfill somewhere in Texas because [the thief had] trashed them after achieving her main goal of boosting the car stereo and GPS," the court held that most of the plaintiffs lacked an imminent injury. Id. at 25-28.

Which Costs Are Recoverable?

If there is a substantial risk that harm will occur, plaintiffs may be able to recover the costs incurred to mitigate or avoid that harm. Courts have held that out-of-pocket expenses for credit reports and credit monitoring are recoverable. See, e.g., *Remijas*, 794 F.3d at 692. Some courts have also suggested that the time spent re-setting accounts and resolving unauthorized accounts may able be compensable, even when it is unclear that plaintiffs incur out-of-pocket costs in taking these steps. See, e.g., id.

But these decisions are not a green light for plaintiffs' counsel. The cases make it clear that plaintiffs "cannot manufacture standing" by accruing unreasonable mitigation costs, *Clapper*, 133 S. Ct. at 1151, or by continuing to accrue mitigation costs after the risk has dissipated. *Whalen v. Michael Stores*, 153 F. Supp. 3d 577, 580-81 (E.D.N.Y. 2015) (finding plaintiff's claimed injury for "lost time and money associated with credit monitoring and other mitigation expenses" was insufficient to confer standing once she "cancelled her affected credit card" and "experienced no further unauthorized activity").

More Guidance Is Needed

Courts have been struggling with the standing requirements in data breach cases, and *Spokeo* and *Clapper* have not provided clear standards. The clear obstacle to class action litigation is that many data breach plaintiffs have no out-of-pocket loss, other than the costs they incur in trying to prevent future harm. But there is controversy over whether plaintiffs have standing to recover these costs. Whether that controversy reflects a circuit split or, as we note above, courts wrestling with difficult facts, courts and parties alike would benefit from more guidance.