By Bill Sampson, Al Saikali, and Dan Schwaller

A Changing Legal Landscape and a Few Suggestions for Counsel

Have you ever searched the Internet for your own name? The amount of information can be staggering if not a little jarring.

Where you live and work, your spouse, where you donate time and money—it is all out there. That said, many of us willingly volunteer personal information on the Internet. One of the first search results is probably your Facebook page.

In fact, most of us are comfortable with our presence on the Internet. But certain key information—social security numbers, banking information, passwords—is and ought to be missing. What happens when these keys to your identity end up in the public domain? We become anxious, at least, and quite possibly angry.

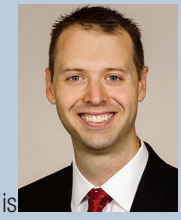
As data breaches proliferate, plaintiffs are demanding action from the courts. Courts do not hesitate to entertain cases where the plaintiffs suffered actual financial loss, but they are divided when the injury is only threatened. When hackers steal personally identifying information ("PII") but have not yet exploited it, the victim may not have standing to sue. "[T]he doctrine of standing serves to identify those disputes which are appropriately resolved through the judicial process." *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990). Should the courts wait until a plaintiff has suffered actual, economic loss from identity theft or fraud? Or, does the mere threat of future harm justify judicial intervention? This article addresses the doctrine of standing, how courts across the country have applied it, and how in-house and outside counsel use it in their efforts to defend data breach cases.

Recent Data Breach Legal Developments

Standing Basics

Defendants often challenge standing early, particularly when plaintiffs seek redress for the threat of future injury rather than for one that has already occurred. "Lack of standing is a defect in subject-matter jurisdiction and may properly be challenged under Rule 12(b)(1)." *Wright v. Incline Vill. Gen. Imp. Dist.*, 597 F. Supp. 2d 1191, 1199 (D. Nev. 2009). Article III standing consists of three elements: (1) injury-in-fact, (2) causation, and (3) redressability. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). The injury must be concrete and particularized as well as actual or imminent. *Id.* Conjectural or hypothetical injuries do not suffice. *Id.* The injury must be fairly traceable to the defendant's conduct, and it must be "likely" that a favorable decision will compensate or otherwise rectify the injury. *Id.*





■ Bill Sampson is a partner in Shook, Hardy & Bacon's Kansas City, Missouri, office and a former president of DRI. Al Saikali is a partner in Shook's Miami, Florida, office and leads the firm's data privacy practice group. Dan Schwaller is an associate in Kansas City, Missouri.

The U.S. Supreme Court's Standing Decision in *Clapper*

The Supreme Court addressed the injury-in-fact requirement in *Clapper v. Amnesty International USA*, 133 S.Ct. 1138 (2013), a case many expected to have widespread repercussions in favor of defendants in data breach cases. *See, e.g.,* Rebecca J. Schwartz, *New U.S. Supreme Court Decision Will Likely Impact Data Breach Litigation*, Data Security Law Journal (Mar. 7, 2013), http://www.datasecuritylawjournal.com/2013/03/07/new-u-s-supreme-court-decision-will-likely-impact-data-breach-litigation/; Douglas Meal, *How High Court's Clapper Ruling Will Impact Breach Cases*, Law360 (Mar. 5, 2013, 1:43 PM), http://www.law360.com/articles/420896/how-high-court-s-clapper-ruling-will-impact-breach-cases.

The 2008 amendments to the Foreign Intelligence Surveillance Act of 1978 allowed the government to conduct, subject to certain conditions, "surveillance of individuals who are not 'United States persons' and are reasonably believed to be located outside the United States." *Id.* at 1140. Amnesty International challenged the law immediately and argued it had suffered an injury-in-fact fairly traceable to the law "because there is an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted… at some point." *Id.* at 1141. Alternatively, the group urged it had standing because "the risk of… surveillance requires them to take costly and burdensome measures to protect the confidentiality of their communications." *Id.*

The Supreme Court rejected Amnesty International's position. *Id.* at 1143. While Amnesty International relied on the Second Circuit Court of Appeals' standard—the threat of a future injury confers standing when there is an "objectively reasonable likelihood" that the injury will occur—the Supreme Court held a threatened future injury must be "certainly impending" to confer standing. *Id.* at 1147. To suffer the actual injury that Amnesty International feared, a chain of five events would need to occur, some of which depended on the independent actions of third parties. *Id.* at 1148. The Court held this chain of possibilities was too attenuated and speculative to satisfy the "certainly impending" standard. *Id.* The Supreme Court rejected Amnesty's alternative argument on the same basis, holding that "costly and burdensome measures" to avoid future harm cannot confer standing when "the harm respondents seek to avoid is not certainly impending." *Id.* at 1151. "If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Id.*

If *Clapper* appeared to close the door to standing in data breach cases where there was no actual injury, it did not take long for other courts to find open windows.

If *Clapper* appeared to close the door to standing in data breach cases where there was no actual injury, it did not take long for other courts to find open windows. First, *Clapper*'s peculiar, five-link chain of events gave courts ample room to distinguish their cases. Second, *Clapper* offered a footnote that seemed to dilute the demanding "clearly impending" standard: "Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur…." *Id.* at 1150, fn 5. Two and a half years later, several courts led by the Seventh Circuit Court of Appeals have moved past *Clapper* to recognize standing in data breach cases where plaintiffs had yet to suffer any actual injury. *See, e.g., In re Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015). *See also Tabata v. Charleston Area Med. Ctr.*, 233 W. Va. 512 (2014) (holding that, under West Virginia law, patients have a legal interest in keeping their medical information confidential.).

That said, other data breach decisions, both pre- and post-*Clapper*, have regularly resulted in dismissal on standing grounds. *See, e.g., In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *5 (N.D. Ill. Sept. 3, 2013); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094–95 (N.D. Cal. 2013); *Willingham v. Global Payments, Inc.*, No. 12-CV-01157, 2013 WL 440702, at *19–20 (N.D. Ga. Feb. 5, 2013); *Hammond v. The Bank of New York Mellon Corp.*, No. 08-civ-6060, 2010 WL 2643307, at *2, 7, 8 (S.D.N.Y. June 25, 2010); *Allison v. Aetna Inc.*, No. 09-2560, 2010 WL 3719243, at *4–6 (E.D. Pa. Mar. 9, 2010); *Randolph v. ING Life Ins. and Annuity Co.*, 486 F. Supp. 2d 1, 4, 7–8 (D.D.C. 2007); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 689-90 (S.D. Ohio 2006). Through the first ten months of 2015, courts in the Northern District of California and the Southern District of Texas continue to disagree with decisions like *In re Adobe* and *Neiman Marcus*. *See, e.g., Antman v. Uber Techs., Inc.*, No. 3:15-cv-01175-LB, 2015 WL 6123054 (Oct. 19, 2015); *Peters v. St. Joseph Svcs. Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015). While defendants have ample case law to support dismissal of data breach cases due to lack of standing, in-house and defense counsel must know the legal landscape to appreciate how courts may reach such differing understandings of *Clapper*.

Competing Interpretations of *Clapper*: *In re Adobe* and *Neiman Marcus* vs. *In re Zappos*, *Galaria*, and *eBay*

In re Adobe Systems, Inc. Privacy Litigation, 66 F. Supp. 3d 1197 (N.D. Cal. 2014), arose in the Northern District of California. Adobe's systems were infiltrated for several weeks in 2013. *Id.* at 1206. The hackers accessed Adobe's source code, customer names, login IDs, passwords, mailing and e-mail addresses, and credit card information, which they were able to decrypt while in Adobe's systems. *Id.* at 1207. The hackers posted some of the stolen data on the Internet; other data was used to exploit vulnerabilities in Adobe products. *Id.* at 1215. Based on these facts, the plaintiffs—Adobe customers—alleged they suffered an injury-in-fact through an increased risk of future harm and costs to mitigate the risk of future harm. *Id.* at 1211. Relying on

numerous district court data breach cases post-*Clapper*, Adobe insisted *Clapper* had resolved that an "increased risk of future harm" was "insufficient to confer Article III standing under the 'certainly impending' standard." *Id.* at 1212.

Unwilling to conclude *Clapper* brought "the sea change that Adobe suggests," *Id.* at 1214, the Northern District chose to distinguish *Clapper*. *Id.* Acknowledging plaintiffs could not supply any evidence their communications had been or would be monitored, requiring a tenuous sequence of events before any actual harm could occur, the court nevertheless observed the hackers stole the *Adobe* plaintiffs' personal information and posted some of the stolen information on the Internet. *Id.* at 1214–15. Whereas *Clapper* presented a risk of harm that was attenuated and speculative and rested on the occurrence of an elongated chain of events, the court felt the risk of harm to Adobe's customers was real and immediate. *Id.* at 1214–15. Citing the *Clapper* footnote, the Northern District held the harm "need not already have occurred or be 'literally certain' in order to constitute injury-in-fact." *Id.* at 1215. Additionally, having found the plaintiffs faced a certainly impending future harm from the theft of their personal data, the court noted plaintiffs' costs to mitigate the damage through credit monitoring services was an additional injury-in-fact for standing purposes. *Id.* at 1207, 1217.

It was during the 2013 holiday season that Neiman Marcus heard its customers were finding fraudulent charges on their bills. *Neiman Marcus*, 794 F.3d at 690. Within a few weeks, the company discovered malware had infected its computer systems and compromised 350,000 credit card numbers. *Id.* Other PII, including social security numbers and birth dates, remained safe. *Id.* By the time the lawsuit arrived in court, identity thieves had used 9,200 cards fraudulently, although all 9,200 cardholders had been fully reimbursed. *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 690–92 (7th Cir. 2015).

Plaintiffs alleged several injuries: an increased risk of future fraudulent charges, lost time and money spent mitigating the damage, and greater susceptibility to identity theft. *Id.* at 692. Neiman Marcus countered that the possibility of future identity theft was too speculative. *Id.* Additionally, because it is standard practice in the credit card industry to reimburse fraudulent charges, Neiman Marcus argued plaintiffs would not suffer any injury even if fraudulent charges appeared on their cards. *Id.*

Distinguishing *Clapper*, the Seventh Circuit felt the risk of identity theft or credit card fraud was "immediate and very real." *Id.* at 693. "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing." *Id.* While the *Clapper* plaintiffs failed to offer evidence of actual government monitoring of their communications, either in the past or in the future, the *Neiman Marcus* plaintiffs established hackers had deliberately targeted Neiman Marcus. *Id.* The *Neiman Marcus* court continued: "Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id.* It used this presumption to find standing for the plaintiffs.

Citing the *Clapper* footnote, the Northern District held the harm "need not already have occurred or be 'literally certain' in order to constitute injury-in-fact."

Neiman Marcus joined *In re Adobe* in its handling of mitigation expenses. *Id.* at 694; *In re Adobe*, 66 F. Supp. 3d at 1207, 1217. The Seventh Circuit observed mitigation expenses can qualify as actual injuries where the harm is imminent, *Neiman Marcus*, 794 F.3d at 694; and it exploited Neiman Marcus's offer of credit monitoring services to each of its affected customers, observing: "It is unlikely that [Neiman Marcus offered these credit monitoring services] because the risk is so ephemeral that it can safely be disregarded." *Id.*

While the *Neiman Marcus* and *In re Adobe* courts found certainly impending future harm in data breach cases, many other courts have not. In January 2012, hackers breached online retailer Zappos' servers and stole customer names, account numbers, passwords, mailing and e-mail addresses, phone numbers, and the last four digits of customer credit cards. *In re Zappos.com, Inc.*, No. 3:12-cv-00325-RCJ-VPC, 2015 U.S. Dist. LEXIS 71195, at *5–6 (D. Nev. June 1, 2015). There, too, plaintiffs alleged their increased risk of identity theft or other fraud constituted an injury-in-fact. *Id.* at *9. Zappos argued plaintiffs lacked standing because they pleaded no actual damage. *Id.*

At this point, the scenario looks familiar: hackers breach the servers, sensitive customer information is lost, and customers sue over the threat of future fraud and identity theft. In *In re Zappos*, though, the details took a modest turn, which changed the outcome of the case. At the time of that breach, the hackers were able to view only the last four digits of the customers' credit cards. *Id.* at *27. Also important, plaintiffs did not allege the identity thieves misused their personal information in any way. *Id.* at *22. Both of these facts weighed against a finding of certainly impending harm. *Id.* at *23. The most important detail in the court's view, however, was the three and a half years that passed between the breach and the legal issues being submitted to the court. *Id.* A series of delays occurred after the data breach, including a motion to compel arbitration, amending the complaint twice, and attempts to mediate. *Id.* at *6–7. Despite such an abundance of time to collect and report evidence of identity theft and fraud, the plaintiffs could not produce a single instance. *Id.* at *23. In the court's mind, "[e]ven if Plaintiffs' risk of identity theft and fraud was substantial and immediate in 2012, the passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something." *Id.* For *In re Zappos*, it meant granting the motion to dismiss. *Id.* at *35. "The more time that passes without the alleged future harm actually occurring undermines any argument that the threat of that harm is immediate, impending, or otherwise substantial." *Id.* at *24–25.

In 2014, the Southern District of Ohio weighed in and dismissed a data breach case due to lack of standing. *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014). Hackers infiltrated Nationwide Mutual Insurance Company's systems in 2012, compromising the plaintiffs' PII. *Id.* at 650. The plaintiffs sued Nationwide on behalf of a class and claimed an increased risk of harm and increased costs to mitigate the risk. *Id.* at 653. Interpreting *Clapper*, the *Galaria* court stated that "an increased risk of identity theft, identity fraud, medical fraud or phishing is not itself an injury-in-fact because Named Plaintiffs did not allege—or offer facts to make plausible—an allegation that such harm is 'certainly impending.'" *Id.* at 654. Even if a data breach increases their likelihood of identity theft, "a factual allegation as to how much more likely they are to become victims than the general public is not the same as a factual allegation showing how likely they are to become victims." *Id.* The Ohio court used Nationwide's offer of free credit monitoring and identity theft protection as a reason to reject finding certainly impending harm. *Id.*

The Eastern District of Louisiana dismissed a data breach case for lack of standing in 2015. *Green v. eBay Inc.*, No. 14-1688, 2015 WL 2066531 (E.D. La. May 4, 2015). After eBay suffered a data breach in 2014, certain customers alleged an increased risk of future identity theft. *Id.* at *4. Relying on *Clapper*, the court held the plaintiff failed to allege any actual or imminent harm. *Id.* at *6. The Eastern District of Louisiana went on to list several factors that help a court ascertain whether plaintiffs suffered actual harm: "whether their data was actually taken when it was accessed, whether certain information was decrypted, whether the data was actually misused or transferred to another third party and misused, and whether or not the third party succeeded in misusing the information." *Id.* at *5. Reasoning "[t]he mere fact that Plaintiff's information was accessed during the Data Breach is insufficient to establish injury-in-fact," *Id.*, the Ohio court dismissed the case for lack of standing. *Id.* at *6.

Suggestions for Corporate and Defense Counsel in Litigation

Standing is an important tool in the toolkit. The recent cases tell us the "certainly impending" standard for future harm can sit lightly on the facts. Success in litigation after a data breach may turn on which types of information the hackers accessed and whether and how rapidly the hackers exploited that information.

Success in litigation after a data breach may turn on which types of information the hackers accessed and whether and how rapidly the hackers exploited that information.

No matter how a data breach happens—malware infections, loss or theft of a company laptop, misdirecting an e-mail, etc.—comprehensive training programs on data security for employees can reduce or eliminate the threat of data breach losses. In *Krottner v. Starbucks Corp.*, the plaintiff filed a class action complaint after an employee's laptop was stolen. 628 F.3d 1139, 1140 (9th Cir. 2010). The laptop contained unencrypted employee information, including names, addresses, and social security numbers. *Id.* Taking note the information was unencrypted, the *Krottner* court held the threat of future harm was certainly impending and plaintiffs had sufficiently alleged an injury-in-fact for Article III standing purposes. *Id.* at 1143. Similarly, the plaintiff in *Polanco v. Omnicell, Inc.* filed a class action complaint after an employee's laptop containing unencrypted medical patient information was stolen from the employee's car. 988 F. Supp. 2d 451, 457 (D. N.J. 2013). The court granted Omnicell's motion to dismiss after determining this particular plaintiff's medical information was not actually on the stolen laptop. *Id.* at 469. *See also Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1322 (11th Cir. 2012) (denying defendant's motion to dismiss after an unencrypted AvMed laptop was stolen and plaintiffs suffered identity theft within 14 months of the theft.).

Like *Krottner* and *Polanco*, most data breach lawsuits arise from a factual scenario that involves human error. *See* Frank Ohlhorst, *IBM Says Most Security Breaches Are Due to Human Error*, Tech Republic (Oct. 8, 2014, 9:17 AM), http://www.techrepublic.com/article/ibm-says-most-security-breaches-are-eue-to-human-error/. Whether an employee loses a device, misdirects an e-mail, clicks on an e-mail or a link that allows malware to infect the system, or intentionally causes a breach, training can help minimize the risks. Businesses can focus on safe storage of sensitive information, training to identify suspicious e-mails and links and create strong passwords, particularly on mobile devices. *See Provide Cyber Security Training for Employees*, Travelers.com, https://www.travelers.com/prepare-prevent/protect-your-business/cyber-security/employee-training.aspx.

Encryption provides an important second layer of security. Just as a locked safe can keep a burglar from stealing a homeowner's most valuable possessions, encryption can keep a hacker from being able to exploit the sensitive information they obtain.

Encryption software scrambles data according to an algorithm. Anyone in possession of the encryption key can descramble the algorithm to determine the actual credit card number. *See What is Encryption?,* Microsoft.com, http://windows.microsoft.com/en-us/windows/what-is-encryption#1TC=windows-7. In the *Krottner, Polanco,* and *AvMed* cases, the information on the employee laptops was unencrypted, allowing the laptop thief access to all sensitive information on the device. *See* 628 F.3d at 1140; 988 F. Supp. 2d at 457. In *In re Adobe*, the hackers encountered encrypted information, but allegedly had access to the encryption key in the same computer system. 66 F. Supp. 3d at 1215.

Encrypting sensitive information and sequestering the encryption key renders the encrypted information worthless to a hacker. Point-to-point (P2P) encryption is

Data Breach › page 83

Data Breach ❮ page 14
gaining popularity because it allows merchants to accept payment without ever taking possession of the sensitive information. The credit card information is encrypted from the consumer all the way to the credit card issuer; the merchant gets paid but never sees the consumer's sensitive information.

Conclusion

In-house and defense counsel have a powerful tool in the standing doctrine. *Clapper's* "certainly impending" standard raised the bar for plaintiffs. But courts around the country recognize plaintiffs can still develop favorable facts. *In re Adobe* and *Neiman Marcus* tell us unencrypted PII and access to complete credit card numbers help plaintiffs show certainly impending harm. In both cases, the plaintiffs were also able to provide evidence of dissemination and misuse. *In re Zappos*, *Galaria*, and *eBay*, on the other hand, show how strong data security thwarted misuse of consumer information and led to the quick dismissal of data breach lawsuits.

Counsel need to consider the standing cases when advising their clients how to respond to breaches. Where incomplete credit card information is obtained, for example, or where the information obtained is encrypted and the encryption key remains secure, an offer of credit monitoring may not be the right move. *Neiman Marcus* is a good reminder of that.

Standing is powerful because it can be applied early and decisively. For data breach cases where plaintiffs have not yet suffered economic loss, *Clapper* set a helpful standard with its requirement that harm be "certainly impending." While not an absolute bar to the lawsuit, it's a good place to start.