COVINGTON

Standing in Data Breach Cases: A Review of Recent Trends

Published in the Bloomberg BNA Class Action Litigation Report on September 25, 2015.

By Simon J. Frankel, Robert D. Fram, Amanda C. Lynch

For most substantial companies, it is said, experiencing a data breach is not a matter of "if," but "when." Particularly when a company is consumer-facing, any publicized data breach is likely to be followed by consumer class action lawsuits.

For several years, Covington and other litigation defense teams have succeeded in obtaining dismissals of class action privacy and security lawsuits at an early stage because named plaintiffs have failed to prove sufficient actual harm to merit standing to sue. And we are engaged in briefing how the law of standing will be addressed by the U.S. Supreme Court in its next term in the case of *Robins v. Spokeo Inc.*, 742 F.3d 409 (9th Cir.2014), cert. granted, 135 S. Ct. 1892 (U.S. Apr. 27, 2015) (No. 113-1339).[1]

This article addresses how courts approach standing in data breach cases following the Supreme Court's decision in *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013), and analyzes which alleged injuries are more likely to be durable in the face of a motion to dismiss. In particular, it focuses on recent high profile cases, such as the Neiman Marcus, Sony and Target litigations, in which motions to dismiss brought on standing grounds were denied (at least in part).

Recent cases reveal a spectrum of harms allegedly suffered by consumers, ranging from the concrete to the more hypothetical. This article divides recent data breach cases into three points along that spectrum, in order of decreasing concreteness: (a) allegations of financial harm resulting from identity theft enabled by the breach; (b) allegations of identity theft but not financial harm; and (c) allegations that the plaintiffs are at an increased risk of future identity theft.[2]

Courts sometimes hold that plaintiffs have standing when they fall into the first or second category, though whether reimbursement of the costs associated with a breach neutralizes standing is a live issue. The major debate concerns the third category: exposure to an increased risk of identity theft. The majority of district courts in reported cases have concluded that increased risk alone cannot meet the injury-in-fact requirement necessary for a federal lawsuit. Nonetheless, a few recent highly publicized decisions have taken a different approach.

---

[1] In Spokeo, the Supreme Court is currently considering whether violation of a statute alone can constitute sufficient injury to create Article III standing in in the context of a privacy claim. Depending on how broadly the Court addresses standing principles, the Court's decision in that case may have implications for the subject of this article.

[2] In these cases, plaintiffs also typically plead an increased risk of financial harm.

In particular, the Seventh Circuit's recent decision in Neiman Marcus carefully compared the Clapper respondents' allegations to the allegations of those affected by acknowledged corporate data breaches. It focused on the fact that, unlike the situation in a national security surveillance case, the plaintiffs in a commercial data breach case often are fully aware of the information that has been improperly accessed, how it has been used, and the costs that have been incurred as a result. Accordingly, the Seventh Circuit concluded that the alleged risks of injury in that case were more transparent and much less speculative.

I. Standing Basics and Clapper

To establish Article III standing in federal court, a plaintiff must show 1) an injury-in-fact; 2) a "sufficient causal connection between the injury and the conduct complained of;" and 3) "a likelihood that the injury will be redressed by a favorable decision." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). To meet the injury-in-fact requirement, a plaintiff must present an injury that is "concrete and particularized and actual or imminent, not conjectural or hypothetical." Id. (internal quotation marks omitted).

In Clapper, the respondents—attorneys and labor, media, and human rights organizations—argued that they had standing based on the "objectively reasonable likelihood" that their sensitive communications with foreign contacts would be monitored under Section 702 of the Foreign Intelligence Surveillance Act. 133 S. Ct. at 1143. The Court rejected this argument, holding that the respondents' allegations that their communications would be intercepted were "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'" Id. (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). Concluding that actual harm relied on a "highly attenuated chain of possibilities," the Court likewise rejected the respondents' other standing theory, premised on the "costly and burdensome measures" they had taken to protect the confidentiality of their communications. Id. at 1148, 1151. The Court held that "respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." Id. at 1151.

The cases discussed below address the fallout from corporate data breaches resulting from hacking, point-of-sale attacks, or hardware theft.[3] In a typical case, a class of data breach victims sues, alleging some combination of actual identity theft, adverse financial consequences, and an increased risk of future identity theft.[4] Consumers' ability to sue in the wake of a corporate data breach was unsettled even before the Supreme Court's decision in *Clapper*. See, e.g., *Reilly v. Ceridian Corp*., 664 F.3d 38 (3d Cir.2011) (holding that alleged increased risk of future harm was insufficient to establish Article III standing); *Krottner v. Starbucks Corp*., 628 F.3d 1139 (9th Cir.2010) (holding that allegations of a credible threat of future harm were sufficient to establish standing); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629

[3] This article discusses only federal data breach cases. State courts are also wrestling with these issues. See, e.g., *Maglio v. Advocate Health & Hosps. Corp.*, 2015 Ill. App. 2d 140782-U (Ill. App. Ct. 2d Dist. 2015); *Tabata v. Charleston Area Med. Ctr.*, 759 S.E.2d 459 (W. Va. 2014).

[4] Courts are not often precise about what exactly they mean by identity theft. Gaining access to a network does not by itself suffice. Identity theft requires active misuse—from hacking an e-mail account to using a social security number to apply for a loan—but does not necessarily include negative financial consequences. This definition includes what is sometimes called "identity fraud," as well as fraudulent credit card use.

(7th Cir.2007) (same). Many courts have since considered Clapper's implications in the data breach context. The majority of district courts have found no meaningful distinction from a standing perspective between the facts alleged in Clapper and the increased risk of future harm that data breach victims plead. Others, including the Seventh Circuit, conclude that Clapper is not dispositive given the factual differences between that case and the data breach cases now before the courts.

II. Standing in Data Breach Cases

Plaintiffs in data breach cases allege a variety of injuries, that can be understood to fall on a spectrum from the most immediate to the more speculative: (a) existing financial injuries, (b) actual misuse of information that may fall short of specific financial injuries, and (c) the alleged near-term risk of the misuse of information.

A. Actual Financial Injury

When plaintiffs can show adverse financial consequences resulting from a data breach, courts typically hold that plaintiffs have alleged an injury-in-fact. Even at the motion to dismiss stage, however, the question of whether the plaintiff is subject to reimbursement for such financial losses has been considered in determining whether the motion should be granted.

1. Alleged Financial Harm

Data breach litigation is not unique in that demonstrated financial injuries typically confer Article III standing. For example, in In re Target Corp. Customer Data Security Breach Litigation, the Minnesota federal district court concluded that customers whose payment card information had been stolen had standing to sue Target. 66 F. Supp. 3d 1154 (D. Minn. 2014). Many of the 114 named plaintiffs in the lawsuit alleged concrete financial harms, including:

- unlawful charges;
- restricted or blocked access to bank accounts;
- inability to pay other bills; and
- late payment or new credit card fees.

Id. at 1159. The court held that this was "sufficient at this stage to plead standing," without examining whether plaintiffs had been reimbursed for these costs. Id.

In Tierney v. Advocate Health and Hospitals Corp., a federal district court in Illinois concluded that the majority of plaintiffs, who had alleged only an increased risk of identity theft, did not have standing because they could not show that harm was certainly impending. No. 13 CV 6237 (N.D. Ill. Sept. 4, 2014). However, the two named plaintiffs who alleged fraudulent account activity were granted standing.

And in *In re Hannaford Brothers Co. Customer Data Breach Litigation*, the federal district court in Maine did not dispute the standing of victims of a point-of- sale breach. 293 F.R.D. 21, 35 (D. Me.2013). The plaintiffs had alleged that 1,800 fraudulent credit- and debit-card charges had

already occurred, and the First Circuit had limited the class to Hannaford customers who had incurred out-of-pocket mitigation costs like card-replacement fees and purchase of credit monitoring and identity theft insurance.5 Id. at 24; see also *Resnick v. AvMed*, 693 F.3d 1317 (11th Cir.2012) (holding that plaintiffs who alleged actual identity theft and monetary damages had standing); *Dolmage v. Combined Ins. Co. of America*, No. 14 C 3809 (N.D. Ill. Jan. 21, 2015) (assuming without discussing that plaintiff who alleged that a false tax return had been submitted and fraudulent T-Mobile and medical charges were incurred in her name had Article III standing).

2. How Reimbursement Affects Determinations

Even an allegation that plaintiffs suffered financial harm as a result of a breach will sometimes fail to establish standing if the plaintiff cannot demonstrate that he or she actually bore that cost.[6] For example, in *Lewert v. P.F. Chang's China Bistro*, the named plaintiff's allegations that another person had attempted to fraudulently charge his account in the wake of a data breach could not confer standing because he did not have to pay monetary damages. No. 14-cv-4787 (N.D. Ill. Dec. 10, 2014). The court concluded that "[i]n order to have suffered an actual injury, Plaintiffs must have had an unreimbursed charge on their credit or debit cards," and rejected all of the plaintiff's other claims of increased risk of identity theft, overpayment, opportunity costs, and mitigation damages; see also *Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1284-85 (N.D. Ala.2014); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617 (N.D. Ill. Sept. 3, 2013).

However, the Seventh Circuit in *Remijas v. Neiman Marcus Group* concluded that even the 9,200 plaintiffs who were later reimbursed for fraudulent charges had alleged an injury-in-fact. Because these 9,200 victims had "suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges," the court was satisfied that they had standing. No. 14-3122 (7th Cir. July 20, 2015). These "identifiable costs associated with the process of sorting things out" were sufficient to show actual harm for those who had already experienced fraudulent charges. The Seventh Circuit's willingness to recognize the incidental costs associated with a data breach may bode well for future plaintiffs whose credit card information is compromised.

Courts might also consider reimbursement at a later stage in the litigation, an approach demonstrated by the Target court. Though not all plaintiffs had alleged they had unreimbursed charges, the court concluded that allegations of financial harm were "sufficient at this stage to plead standing." 66 F. Supp. 3d at 1159.

B. Actual Identity Theft But No Financial Harm

When plaintiffs can allege specific facts indicating that their information was not only accessed but also misused by a third party, they can generally establish standing even without showing financial harm. For example, in *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, several data tapes containing the personal information and medical

---

[5] The U.S. District Court for the District of Maine ultimately refused to certify the class under Rule 23(b), concluding that the plaintiffs failed to show predominance of common questions of law or fact. Id. at 30-33.

[6] While courts typically consider the issue of reimbursement as part of the injury-in-fact requirement, it might also properly be considered as part of the redressability analysis.

records of 4.7 million members of the U.S. military and their families were stolen from a car. 45 F. Supp. 3d 14 (D.D.C.2014). The D.C. federal district court concluded that the vast majority of the victims of the data breach, who alleged only that their data had been stolen, should be dismissed from the case for failing to meet the injury-in-fact requirement. Id. at 19. However, two plaintiffs who plausibly alleged that their data was "accessed or abused" had asserted the necessary injury-in-fact. Id. One of those plaintiffs began receiving unsolicited telephone calls pitching medical products and services targeted at her specific medical condition, a record of which was stored on the tape. Id. at 33. The other alleged that he received mail indicating that he had applied for a loan that he did not apply for, and that his credit history had been adversely affected as a result. Id. at 32. The court declined to extend their plausible allegations to the group at large, holding that their individual experiences did not "lead to the conclusion that wide-scale disclosure and misuse of all 4.7 million TRICARE customers' data is plausibly 'certainly impending.'" Id. at 34.

In *Corona v. Sony Pictures Entertainment, Inc.*, allegations that plaintiffs' information had been stolen, posted on file sharing sites, and used to send threatening e-mails to former Sony employees and their families were sufficient to confer standing. No. 14-CV-09600 RGK (C.D. Cal. June 15, 2015). The Central District of California concluded that "[t]hese allegations alone" were sufficient.[7]

As *Green v. eBay* demonstrates, however, conclusory allegations that all class members have suffered identity theft likely will not suffice. No. 14-1688 (E.D. La. May 4, 20145). There, eBay suffered a data breach in 2014, and eBay users filed a class action alleging that the plaintiff and putative class members had suffered actual identity theft. The court refused to find standing on these grounds, noting that the plaintiff had not alleged specific facts indicating that any class member had suffered identity theft. Because the plaintiff failed to allege a concrete and particularized injury that was certainly impending, the court held that the plaintiff had not adequately alleged an injury-in-fact. *See also Burrows v. Purchasing Power*, No. 1:12-cv-22800-UU (S.D. Fla.Oct. 18, 2012) (holding that actual identity theft confers standing independent of financial harm); *Badish v. RBS Worldpay, Inc.*, No. 1:09-CV-0033-CAP (N.D. Ga. Feb. 5, 2010) (holding that a plaintiff who alleged actual identity theft had standing, while a plaintiff who alleged only exposure of information did not).

C. Elevated Risk of Future Identity Theft

The most commonly alleged injury in the wake of a data breach is an increased risk of future identity theft. Predictably, it is here that courts grapple most directly with *Clapper*. Differences in a given jurisdiction's precedent appear to explain some outcomes, while factual particularities determine others.

1. Courts Refusing to Hold that Increased Risk From a Breach Is Sufficient to Confer Standing

In a typical data-breach case, plaintiffs who have not yet experienced actual misuse of their data will argue that, as a result of the breach, they are now at an increased risk of identity theft.

[7] Although the court characterized plaintiffs' allegations as a credible threat or certainly impending injury, the fact that the information had not only been accessed but published and used to contact the employees makes these allegations one step more concrete than the pure risk cases discussed below.

The company that was breached will then move to dismiss, contending that the plaintiffs cannot meet Clapper's "certainly impending" standard. In the majority of cases, district courts have agreed with the company, concluding that proof that the company's system was breached (either by hacking, point-of-sale attacks, or hardware theft) is not equivalent to a "certainly impending" risk of harm. See Appendix A (listing cases).

Plaintiffs have several times sought to demonstrate their elevated risk of future identity theft by citing the statistic that an individual who has been the victim of a data breach is 9.5 times more likely to become the victim of identity theft. This approach has not been successful, as courts view this statistic as evidence of a low absolute risk of becoming a victim of identity theft, even if plaintiffs' relative risk is somewhat higher than the average person's. Several courts have accordingly concluded that identity theft is not certainly impending, and therefore that plaintiffs do not have standing. See, e.g., *SAIC*, **45 F. Supp. 3d 14, 26** (D.D.C.2014) ("By Plaintiff's own calculations, then, injury is likely not impending for over 80% of victims."); *Green v. eBay*, No. 14-1688 (E.D. La. May 4, 2015); *Galaria v. Nationwide Mut. Ins. Co.*, **998 F. Supp. 2d 646, 654** (S.D. Ohio 2014); *Strautins v. Trustwave Holdings, Inc.*, **27 F. Supp. 3d 871, 877** (N.D. Ill. 2014).

If the increased risk of harm is not itself considered sufficiently imminent, courts will also hold that costs expended to mitigate that risk do not establish an injury-in-fact. See, e.g., *Remijas v. Neiman Marcus Group*, No. 14-3122 (7th Cir.July 20, 2015) ("Mitigation expenses do not qualify as actual injuries where the harm is not imminent."); *SAIC*, 45 F. Supp. 3d at 26 ("Nor is the cost involved in preventing future harm enough to confer standing, even when such efforts are sensible.").[8]

2. Cases Finding Standing Based on an Increased Risk of Future Identity Theft

The Seventh Circuit and a handful of other courts have held that increased susceptibility to future injury can constitute an injury-in-fact, distinguishing Clapper on factual or policy grounds.

a. Remijas v. Neiman Marcus Group

In the recent case Remijas v. Neiman Marcus Group, the Seventh Circuit carefully distinguished the impending harms alleged in Clapper from the harms alleged in the data breach case before it. 350,000 payment cards were potentially exposed to malware that infiltrated Neiman Marcus's computer systems. 9,200 of those cards were known to have been used fraudulently. After

[8] Untimely notice of the data breach also typically does not confer standing unless the plaintiffs can show a separate, incremental harm that resulted from the delay. See *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK (C.D. Cal. June 15, 2015) (holding that, while the consequences of the data breach gave plaintiffs standing to sue, delayed notice did not itself confer standing); In re *Adobe Sys. Privacy Litig.*, No. 13-CV-05226-LHK (N.D. Cal. Sept. 4, 2014) (same); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617 (N.D. Ill. Sept. 3, 2013) (holding that delayed notice in violation of a state statute could not independently confer standing absent actual damages). However, the Minnesota district court granted that plaintiffs would have standing under state data-breach notice statutes if they could show that they would not have shopped at Target had they been timely notified about the breach. *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1166 (D. Minn. 2014). The case settled before the "would not have shopped at Target" theory could be tested following the pleadings.

concluding that those 9,200 plaintiffs had standing, the court addressed those plaintiffs who had alleged only imminent injuries. In so doing, the court narrowed the effect of Clapper in two ways.

First, the Seventh Circuit reiterated that Clapper "did not jettison the 'substantial risk' standard" for standing based on future injuries. The Court thereby clarified that the basic rules of Article III standing were not changed by Clapper.

Second, and perhaps most importantly, the Seventh Circuit stated that the plaintiffs in a data breach case are very differently situated than the plaintiffs in a national security surveillance case. In particular, the victims of the Neiman Marcus breach needed to speculate about neither whether their information had been stolen nor what information had been taken. In contrast, the Clapper plaintiffs provided "no evidence that any of respondents' communications either had been or would be monitored."

In following this line of thought, the Seventh Circuit expressly built on another decision that had limited Clapper, the Adobe decision. Likening the case to one in which Adobe was "deliberately targeted" by hackers, the court held that there was an "objectively reasonable likelihood" that identity theft would occur and therefore that plaintiffs had standing; "Why else would hackers break into a store's database and steal consumers' private information?"

Finally, since the harm alleged by the data breach victims was sufficiently imminent, the costs they expended to protect themselves from that harm constituted an additional injury-in-fact. Noting that Neiman Marcus's offer of one year of credit monitoring and identity-theft protection was "telling," the court concluded that the costs of these services "easily qualifie[d] as a concrete injury." The plaintiffs also alleged that they overpaid for the products they purchased from Neiman Marcus and that they lost their private information, an intangible commodity. Though the court found these theories "dubious," it ultimately did not decide whether the plaintiffs' two remaining standing theories would have sufficed.

b. District Court Cases in the Ninth Circuit

A number of courts in the Ninth Circuit have read *Clapper* to be consistent with prior precedent holding that an increased risk of future harm in the data breach context was sufficient to confer standing. These courts have expressly found that the facts of data breach cases can be harmonized with the standing principles articulated in Clapper and/or narrowed *Clapper* to the national security context in which it arose.

For example, in *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, the federal district court for the Southern District of California determined that Clapper need not overrule prior Ninth Circuit precedent, citing *Krottner v. Starbucks Corp.*, **996 F.Supp. 2d 942** (S.D. Cal. 2014). Holding that "Clapper did not set forth a new Article III framework," the Southern District concluded that the plaintiffs, Sony customers whose personal information had been stored on Sony's network, had alleged a "'credible threat' of impending harm" by pleading that hackers had accessed their information. Id. at 962.

Similarly, the Northern District of California concluded in *In re Adobe Systems Privacy Litigation* that *Clapper* "did not overrule any precedent, nor did it reformulate the familiar standing requirements." **66 F. Supp. 3d 1197, 1213** (N.D. Cal. 2014). In addition to noting the Supreme Court's failure to announce a sweeping doctrinal change, the Northern District observed that *Clapper* arose in the "sensitive context of a claim that other branches of government were

violating the Constitution." Id. at 1214. After concluding that Krottner and *Clapper* were not "clearly irreconcilable," the Northern District further held that plaintiffs' allegations were "sufficiently concrete and imminent to satisfy *Clapper*," because there was no need to speculate as to whether the plaintiffs' information had been stolen by someone who intended to misuse, and was capable of misusing, their data. Id. at 1214-15. The court noted that some of the stolen information had already surfaced on the Internet, and that the hackers had used Adobe's own systems to decrypt credit card numbers, such that harm was "certainly impending." Because plaintiffs faced a substantial risk of future harm, their allegations relating to the cost of mitigating this risk constituted an additional cognizable injury. Id. at 1216-17.

Nevertheless, a decision by the U.S. District Court for the District of Nevada demonstrates the limits of the Ninth Circuit's arguably looser standard. In *In re Zappos.com, Inc.*, a group of customers who alleged that some of their personal information—account numbers, passwords, names, email and mailing addresses, phone numbers, and the last four digits of their payment cards—was exposed by Zappos were not held to have standing. No. 3:12-cv-00325- RCJ-VPC (D. Nev. June 1, 2015). While agreeing that *Krottner* remained the most relevant precedent, the court concluded that here, the increased risk of future harm was neither substantial nor imminent. The court reasoned that years had passed since the breach, none of the stolen information had yet surfaced on the Internet, the information stolen was less sensitive and did not in itself enable fraudulent charges, and the value of the goods plaintiffs purchased from *Zappos* was in no way affected by the breach.

c. Outside the Ninth Circuit

Outside the Ninth Circuit, one court within the Northern District of Illinois has held that Clapper's more rigorous standard is confined to certain contexts. Citing the Seventh Circuit's decision in *Pisciotta v. Old National Bancorp*, the court in *Moyer v. Michaels' Stores, Inc.* distinguished Clapper's admittedly rigorous application of the "certainly impending" standard from that required by the consumer data breach case before the court. No. 14 C 561 (N.D. Ill. July 14, 2014). The court noted that Clapper concerned national security and constitutional issues, a more recent Supreme Court case recited less demanding standards when describing the test for standing conferred by future harm, and the Clapper respondents could not provide any evidence that the relevant risk of harm had ever materialized in similar circumstances. In contrast, the Moyer court was satisfied that the link between a data security breach and identity theft was not speculative or hypothetical, and therefore held that the plaintiffs, victims of a point-of-sale attack on Michaels' craft stores, had standing to sue.

3. Factors Influencing How Courts Assess Risk of Future Identity Theft

Courts often measure the logical distance between the alleged facts and the harm plaintiffs fear, distinguishing those cases in which identity theft is more remote. Two factors courts assess in making this determination are the circumstances of the breach and the length of time that has passed without incident.

a. Chain of Contingencies

Mirroring *Clapper*, many courts evaluate claims arising from data breaches by walking through the "speculative chain of possibilities" required in order for a specific theft to cause actual harm.

133 S. Ct. at 1150. Factors here include the intervening role of third parties and the relative difficulty of using the data in question to effectuate an identity theft of some kind.

The *SAIC* case focused on the number of steps an identity thief would have to take to capitalize on the stolen information. This case concerned backup data tapes containing health and other data that were stolen from a car. The court acknowledged that, for identity theft to occur, the thief would have to 1) recognize what the tapes were; 2) find an appropriate tape reader; 3) attach the tape reader to her computer; 4) acquire software to upload the data from the tapes; 5) decrypt the encrypted portions of the tapes; 6) become familiar with the health insurance company's database format; and 7) actually misuse a particular plaintiff's name and social security number. 45 F. Supp. 3d at 25.

In contrast, the Adobe court proposed a significantly shorter chain. The shortness of the chain here was marked by the fact that the hackers had allegedly:

- targeted Adobe's servers;
- actually collected plaintiffs' personal information;
- already used Adobe's system to decrypt credit card numbers; and
- posted some of the information online.

Thus, on these facts, the only remaining link in the chain was actual abuse of the data. 66 F. Supp. 3d at 1215-16. Crucially, the Adobe court, like the Seventh Circuit in Neiman Marcus, was willing to assume that hackers stole the information for the purpose of misusing it, unlike the thief who broke into the car in SAIC. These cases suggest that effective encryption may persuade courts that the risk of identity theft is sufficiently attenuated to undermine standing.

Courts sometimes focus on the role of independent third parties. In Zappos, for example, the court noted that the "degree of Plaintiffs' speculation is heightened further by the fact that the future harm is based entirely on the decisions or capabilities of an independent, and unidentified, actor." The court highlighted that whoever was in possession of the stolen information could choose not to misuse the data, or might be unable to use the data, such that the "damages at this point rely almost entirely on conjecture." see also, e.g., *Peters v. St. Joseph Servs. Corp.*, No. 4:14-CV-2872 (S.D. Tex. Feb. 11, 2015) ("Peters might be able to demonstrate harm if third parties become aware of her exposed information and reveal their interest in it; if they form an intent to misuse her information; and if they take steps to acquire and actually use her information to her detriment.");

b. Time Between the Breach and Litigation

Another factor counseling against standing is a long period of time between the data breach and resolution of the relevant motions. In Zappos, the court concluded, "perhaps the most distinguishing element between this case and Adobe and Sony is the amount of time from when the breach occurred to when the respective motions to dismiss were ruled upon." Because three-and-a-half years had elapsed between the breach and the court's decision without plaintiffs alleging that they had experienced actual financial harm or dissemination of their private information, the court concluded that plaintiffs could not show the presence of an imminent threat. In another case, *Storm v. Paytime, Inc.*, the court acknowledged that, "even though Plaintiffs may indeed be at greater risk of identity theft, the data breach in this case occurred in April 2014—almost a year ago—and Plaintiffs have yet to allege that any of them

have become actual victims of identity theft." No. 14-cv-1138 (M.D. Penn. Mar. 13, 2015). Such a delay contradicted even lay notions of imminence, the court concluded, and therefore held that the plaintiffs had failed to establish standing.

The Seventh Circuit acknowledged the bind in which this factor can leave plaintiffs. *Remijas v. Neiman Marcus Group*, No. 14-3122 (7th Cir.July 20, 2015). Plaintiffs who move quickly after a breach are less likely to be able to show concrete harms, while those who wait until identity thefts have occurred give the defendant "more latitude … to argue that the identity theft is not 'fairly traceable to the defendant's data breach,'" an issue discussed in more detail below. Id. (quoting In re Adobe Sys.) (internal quotation marks removed).

D. Causation and Redressability

While the injury-in-fact prong of standing most often obstructs plaintiffs' attempts to seek redress following a data breach, causation and redressability can also scuttle data breach litigation.

For example, in *Peters v. St. Joseph's Services Corp.*, the plaintiff alleged fraudulent activity had already occurred in her accounts following a data breach. However, the district court in Texas dismissed this as grounds for standing, holding that *Peters*' complaint "fail[ed] to account for the sufficient break in causation caused by opportunistic third parties." No. 4:14-CV-2872 (S.D. Tex. Feb. 11, 2015). The court further concluded that, even if *Peters*' injuries were fairly traceable to the defendant's actions, her allegations failed the redressability prong because she did not allege any quantifiable damages as a result of the breach, and her credit card company and e-mail provider had already remedied some of her injuries.

In *SAIC*, the D.C. district court dismissed several plaintiffs on causation after they alleged that their personal information was used to make fraudulent purchases. *45 F. Supp. 3d at 31*. Because credit, debit, or bank account information was not on the stolen tapes, the link between the fraudulent charges and the breach was necessarily too attenuated to demonstrate causation. Only the named plaintiff whose personal information had been used to take out a loan and another whose unlisted phone number began receiving solicitation calls targeting a medical condition listed on the stolen tapes could sufficiently demonstrate a causal link. Id. at 32-33.

In the Neiman Marcus case, however, the Seventh Circuit concluded that, for causation purposes, "[i]t is enough at this stage of the litigation that Neiman Marcus admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk." Neiman Marcus had argued that the occurrence of several other large-scale commercial data breaches during the same time frame meant plaintiffs could not show that their injuries were fairly traceable to the Neiman Marcus breach. Regarding redressability, the Seventh Circuit concluded that some of the plaintiffs' harms could be redressed, including any unreimbursed mitigation expenses or future injuries. Because business practices regarding reimbursement vary and because federal law does not require that credit card companies adopt "zero liability" policies, the redressability prong was met for "any injuries caused by less than full reimbursement of unauthorized charges."

III. Conclusion

It increasingly appears that courts engage in a fact-specific analysis of the harms, actual and potential, that victims of a data breach face when determining whether those plaintiffs have standing. The recent Seventh Circuit decision in Neiman Marcus provides some guidance to courts in that circuit, providing a more liberal approach to standing doctrine. On the other hand, most courts to date having held that mere risk of identity theft, without more, is insufficient to provide the basis for standing to sue in federal court. Further development of the case law in this area will clarify the extent to which this harm, the most common effect of data breaches, is cognizable on its own terms.

Appendix A: Federal Data Breach Cases Holding that Plaintiffs Alleging an Increased Risk of Future Harm Did Not Have Standing

Post-*Clapper*

Burton v. MAPCO Express, **47 F. Supp. 3d 1279** (N.D. Ala.2014) (holding that a plaintiff would have standing only if he could allege that he both experienced fraudulent charges and incurred damages)

Galaria v. Nationwide Mut. Ins. Co., **998 F. Supp. 2d 646** (S.D. Ohio 2014) (holding that the risk of identity theft was not certainly impending and therefore that plaintiffs did not have standing, except with respect to state invasion of privacy claims)

Green v. eBay, No. 14-1688 (E.D. La. May 4, 2015) (dismissing plaintiffs' claims for failure to allege an injury-in-fact)

In re Barnes and Noble Pin Pad Litig., No. 12-cv-8617 (N.D. Ill. Sept. 3, 2013) (same)

In re Horizon Healthcare Servs. Data Breach Litig., No. 13-7418 (D.N.J.Mar. 31, 2015) (dismissing plaintiffs' claims for failure to adequately allege injury-in-fact and, in the case of one plaintiff, causation)

In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C.2014) (holding that only those plaintiffs who could show their data had been accessed or abused had standing)

In re Zappos.com, Inc., No. 3:12-cv-00325-RCJ-VPC (D. Nev. June 1, 2015) (holding that the alleged risk of identity theft was neither sufficiently immediate nor substantial enough to confer standing)

Lewert v. PF Chang's China Bistro, No. 14-cv-4787 (N.D. Ill. Dec. 10, 2014) (dismissing plaintiffs' claims for failure to allege an injury-in-fact)

Peters v. St. Joseph Servs. Corp., No. 4:14-CV-2872 (S.D. Tex. Feb. 11, 2015) (same)

Polanco v. Omnicell, **998 F. Supp. 2d 451** (D.N.J. 2013) (same)

Remijas v. Neiman Marcus Group, No. 14 C 1735 (N.D. Ill. Sept. 16, 2014), rev'd, No. 14-3122 (7th Cir.July 20, 2015) (holding that the appearance of fraudulent charges on 9,200 out of

350,000 payment cards did not permit the plausible inference that all plaintiffs were at a "certainly impending" risk of identity theft)

Storm v. Paytime, Inc., No. 14-cv-1138 (M.D. Pa. Mar. 13, 2015) (dismissing plaintiffs' claims for failure to allege an injury-in-fact)

Strautins v. Trustwave Holdings, Inc., **27 F. Supp. 3d 871** (N.D. Ill. 2014) (granting defendant's motion to dismiss for lack of standing because plaintiff failed to allege an "imminent" or "certainly impending" risk that she would be a victim of identity theft or fraud)

Tierney v. Advocate Health & Hosps. Corp., No. 13 CV 6237 (N.D. Ill. Sept. 4, 2014) (holding that only those two plaintiffs who alleged actual fraudulent account activity had standing)

Pre-Clapper

- *Reilly v. Ceridian Corp.*, **664 F.3d 38** (3d Cir.2011) (affirming district court's dismissal of plaintiffs' complaint for failure to allege an injury-in-fact)
- *Allison v. Aetna, Inc.*, No. 09-2560 (E.D. Pa. Mar. 9, 2010) (holding that plaintiffs failed to allege an injury-in-fact)
- *Amburgy v. Express Scripts, Inc.*, **671 F. Supp. 2d 1046** (E.D. Mo. 2009) (same)
- *Bell v. Acxiom Corp.*, No. 06-485 (E.D. Ark. Oct. 3, 2006) (same)
- *Giordano v. Wachovia Sec.*, No. 06-476 (D.N.J. July 31, 2006) (same)
- *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08-6060 (S.D.N.Y. June 25, 2010) (same)
- *Hinton v. Heartland Payment Sys., Inc.*, No. 09-594 (D.N.J. Mar. 16, 2009) (same)
- *Key v. DSW, Inc.*, **454 F. Supp. 2d 684** (S.D. Ohio 2006) (same)
- *Randolph v. ING Life Ins. & Annuity Co.*, **486 F. Supp. 2d 1** (D.D.C. 007) (same)

Robert D. Fram is a litigation partner at Covington & Burling LLP in San Francisco, where he focuses on patent, copyright, trade secret and licensing cases.

Simon J. Frankel is a litigation partner at Covington & Burling in San Francisco, where he focuses on copyright and trademark litigation, Internet privacy and technology disputes.

Amanda C. Lynch was a summer associate at Covington & Burling's San Francisco office in 2015.

If you have any questions concerning the material discussed in this client alert, please contact:

Robert Fram	+1 415 591 7025	rfram@cov.com
Simon Frankel	+1 415 591 7052	sfrankel@cov.com