DAMAGES THEORIES IN DATA BREACH LITIGATION

Paper Authors: Eric S. Boos[*]
Chandler Givens[**]
Nick Larry[***]

I. INTRODUCTION

As of the time of writing, there have been over 600 reported data breaches in 2014 alone, resulting in the exposure of hundreds of millions of personal records.[1] This is a 25 percent increase over 2013, which itself was a 30 percent increase over 2012.[2] These figures do not include the potential hundreds or thousands of additional breaches that go unreported every year, whether willfully or on account of ignorance about the incident.[3] This exponential uptick in data breaches, or at least the increased visibility of such events, has prompted a surge of privacy litigation.

These legal efforts have taken a variety of forms. Generally brought as class actions, individuals seeking redress have relied on common law and statutory (federal and state) privacy rights, as well as state consumer protection laws, in order to establish a viable cause of action. For the most part these cases have failed to progress past the motion to dismiss stage, as defendants have successfully challenged the ability of litigants to demonstrate a cognizable injury sufficient to confer Article III standing. In response, plaintiffs have continued to develop alternative damages theories to demonstrate they have suffered harm. While such theories have

---

[*] Eric is an Attorney with Shook, Hardy & Bacon, LLP's Data Security and Data Privacy Practice Group.
[**] Chandler is an attorney at Edelson PC where he leads the technical research arm of the firm.
[***] Nick is an attorney at Edelson PC.
[1] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.
[2] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html.
[3] Thomas Claburn, *Most Security Breaches Go Unreported*, InformationWeek (July 31, 2008), http://www.darkreading.com/attacks-and-breaches/most-security-breaches-go-unreported/d/d-id/1070576?.

found some success in advancing cases beyond pleading, by-and-large a consistently effective argument remains elusive. After providing a brief overview of standing doctrine as articulated by the federal courts, this paper provides an overview of the judiciary's treatment of such theories to date and closes with a prediction of the near future of damages theories in data breach litigation.

II. EVOLVING DAMAGES THEORIES

A. Article III Standing

Consumers affected by data breaches face significant obstacles when bringing claims in federal court related to the exposure of their personally identifiable information ("PII"). The largest impediment so far has been meeting the standing requirement imposed by Article III of the United States Constitution.[4] To demonstrate Article III standing a plaintiff must show (1) she suffered an "injury in fact;" (2) her injuries were "fairly traceable" to defendant's actions; and (3) that a favorable judgment will redress her injuries.[5] The plaintiff's "injury-in-fact" must be both "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[6] As discussed in Section B, *infra*, Article III requires that a threatened injury must be "certainly impending" to constitute an "injury-in-fact" when an actual injury has not yet occurred.[7] Plaintiffs, having tried and failed to show that they suffered a "concrete and particularized" injury in the form of financial harm, have developed a number of alternative theories to assert standing. The success of these theories has been mixed.

B. Increased Risk of Future Harm.

[4] U.S. Const. art. III, § 2, cl. 1 states "The Judicial Power shall extend to all Cases . . . [and] to Controversies." Article III standing has been interpreted to facilitate both separation of powers and the federal courts' role as courts of limited jurisdiction. *See* Cnty. Court of Ulster Cnty., N.Y. v. Allen, 442 U.S. 140, 154 (1979).
[5] Resnick v. AvMed, Inc., 693 F.3d 1317, 1323 (11th Cir. 2012).
[6] *Id*. (internal citations omitted).
[7] Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1147 (2013).

The most argued alternative theory holds that the plaintiff, having had her PII compromised in a data breach, faces a heightened risk of future harm, e.g., the potential for her data to be exploited by nefarious actors to commit identify theft. In large measure this approach has been rejected. The court in *Galaria v. Nationwide Mut. Ins. Co*. adequately summarized the judiciary's view of the theory as follows: "Even though [plaintiffs] allege a third party or parties have their PII, whether [plaintiffs] will become victims of theft or fraud or phishing is entirely contingent on what, if anything, the third party criminals do with that information. If they do nothing, there will be no injury."[8] Few courts have reached an opposite conclusion.

Few, however, does not mean none. Several courts have found that an increased future risk of harm may, in certain circumstances, constitute sufficient injury to confer Article III standing. *Krottner v. Starbucks Corp.*[9] is the seminal case in this regard. There, a putative class of current and former Starbucks employees sued the ubiquitous coffee shop after a company laptop containing their names, addresses, and social security numbers was stolen. The plaintiffs alleged that their employer's failure to reasonably protect their highly sensitive information was both negligent and a breach of implied contract.[10] The defendant (and the lower court) reasoned that absent any evidence of actual identity theft from the breach, plaintiffs failed to show they suffered economic harm.[11] The Ninth Circuit disagreed, ruling that because of the highly sensitive nature of the improperly accessed information, the plaintiffs faced a "credible threat of real and immediate harm" and therefore satisfied the injury-in-fact requirement for Article III standing because their information was exposed in the data breach.[12]

---

[8] Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 655 (S.D. Ohio 2014) (collecting cases).
[9] 628 F.3d 1139 (9th Cir. 2010).
[10] *Id.* at 1141.
[11] *Id.*
[12] *Id.* at 1143.

The Seventh Circuit considered a similar argument in *Pisciotta v. Old Nat. Bancorp*.[13] Consumers in that case sued their bank following a data breach that resulted in the disclosure of their names, social security numbers, drivers' license numbers, birth dates, mothers' maiden names, credit card, and other financial account numbers.[14] Assessing its own jurisdiction, the Seventh Circuit held that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions" and plaintiffs had standing to sue by virtue of their allegations that the defendant's breach created an increased risk of future harm.[15] Ultimately, however, the Seventh Circuit affirmed the district court's dismissal, finding that while the plaintiffs alleged *injury* in the form of the increased risk of future harm, that increased risk could not constitute the *damages* necessary to maintain their claims.[16]

Conversely, the First, Third, and Sixth Circuits have rejected risk-of-future-harm theories outright, finding no standing under similar facts.[17] This lack of consistency has resulted in a body of data breach case law with varying outcomes and no determinative doctrine. Still, at bottom, the majority of courts to examine this question have ruled that the increased risk of future harm is not enough to establish Article III standing.

Many observers reckoned that the Supreme Court would settle the matter for good with a decision from outside the data breach context, *Clapper v. Amnesty International USA*.[18] Respondents in *Clapper* were attorneys and organizations concerned about becoming subject to government surveillance pursuant to Section 702 of the Foreign Intelligence Surveillance Act of

[13] 499 F.3d 629 (7th Cir. 2007).
[14] *Id.* at 631.
[15] *Id.* at 634.
[16] *Id.* at 640.
[17] *See, e.g.* Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); Lambert v. Hartman, 517 F.3d 433, 436 (6th Cir. 2008).
[18] 133 S. Ct. 1138, 1142 (2013).

1978 ("FISA") [19] because there was "an objectively reasonable likelihood that their communications [would] be acquired [under FISA] at some point in the future." 133 S.Ct. at 1142-46. Despite this allegedly objective likelihood, however, the Court held that the potential harm wasn't certain enough, instead asserting that the "threatened injury must be certainly impending to constitute injury in fact." *Id.* at 1147. In the wake of this decision, data breach defendants have routinely argued that a plaintiff alleging increased risk of future harm must establish the feared harm as "certainly impending" to possess standing.

The strategy has worked, for the most part. Since its publication at least seven courts have cited *Clapper* and its "certainly impending" standard when jettisoning data breach lawsuits for lack of standing.[20] Yet uncertainty about the future viability of the increased risk of future harm theory still lingers after other courts have discarded the notion that *Clapper* somehow altered the standing test.

The Northern District of Illinois, for instance, after noting that at least one of the plaintiffs in *Moyer v. Michaels Stores, Inc.* had already incurred fraudulent charges on her credit card, held that "the elevated risk of identity theft stemming from the data breach at Michaels is

[19] FISA, first enacted in 1978, has repeatedly been amended since the September 11, 2001, terrorist attacks. Section 702 allows the United States Attorney General and Director of National Intelligence, for a period of up to one year, to engage in "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." The Attorney General and Director of National Intelligence must submit an application for an order from a specially created court to conduct such surveillance. *See* 50 U.S.C. § 1881a.

[20] *See* Remijas v. Neiman Marcus Group, LLC, No. 14-C-1735, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014) (victims of credit card data breach lacked standing to sue for increased risk of harm); In re Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) (same); In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., MDL No. 23600, 2014 WL 1858458 (D.D.C. May 9, 2014) (victims of military data breach lacked standing to sue for increased risk of future harm; Strautins v. Trustwave Holdings, Inc., No. 12-C-09115, 2014 WL 960816 (N.D. Ill. Mar. 12, 2014) (plaintiffs lacked standing to sue data security vendor for increased risk of harm arising from hacking incident); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 655 (S.D. Ohio 2014) (collecting cases); Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451 (D.N.J. Dec. 26, 2013) (health care data breach victims lacked standing to sue for increased risk of future harm).

sufficiently imminent to give Plaintiffs standing."[21] Departing from several other post-*Clapper* data breach cases in the Northern District of Illinois,[22] the *Moyer* court reasoned that its conclusion followed from *Pisciotta* and was consistent with prior Supreme Court decisions finding standing based on an imminent risk of future injury. *Moyer* distinguished *Clapper* based on the latter's rigorous application of the "certainly impending" standard in a case that involved (1) national security and constitutional issues and (2) no evidence that the relevant risk of harm had ever materialized in similar circumstances."[23]

In a recent class action arising from the breach of 38 million of Adobe's customers' "names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and e-mail addresses," Judge Koh of the Northern District of California—no stranger to data breach litigation—held:

> In any event, even if *Krottner* is no longer good law, the threatened harm alleged here is sufficiently concrete and imminent to satisfy *Clapper*. Unlike in *Clapper,* where respondents' claim that they would suffer future harm rested on a chain of events that was both "highly attenuated" and "highly speculative," the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real. Plaintiffs allege that the hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates. Plaintiffs' personal information was among the information taken during the breach. Thus, in contrast to *Clapper,* where there was no evidence that any of respondents' communications either had been or would be monitored under Section 702, here there is no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken.[24]

---

[21] Moyer v. Michaels Stores, Inc., No. 14-C-561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014).
[22] *See e.g.* Strautins v. Trustware Holdings, Inc. No. 12-C-9115, 2014 WL 960816, at *4 (N.D. Ill. Mar. 12, 2014); In re Barnes & Noble Pin Pad Litig., No. 12-C-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013).
[23] Moyer, 2014 WL 3511500, at *6.
[24] In re Adobe Sys., Inc. Priv. Litig., 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014).

Critically, the *Adobe* court found that the very fact that hackers had accessed and misappropriated the PII was, in and of itself, sufficient to infer that the injury to plaintiffs was "certainly impending."[25] From this, the court distinguished the host of other post-*Clapper* data breach cases dismissing claims where no evidence of similar malicious actors was presented.[26] Whether other courts will adopt this reasoning and find that the involvement of hackers and other ne'er-do-wells is *prima facie* evidence that injury is imminent remains to be seen.

More generally, it's difficult to predict from these cases how courts will handle the increased risk of harm theory of damages in the future. Extrapolating from *Adobe* and *Michaels Stores*, it seems that the answer will turn on a fact-specific inquiry into the circumstances surrounding the breach and the likelihood of real future harm. Other courts will probably continue to dismiss data breach cases for failing to satisfy *Clapper's* standing requirements.

C. The Dissemination of Personal Information Reduces Its Inherent Value.

Plaintiffs have also attempted to plead damages by asserting that a breach or disclosure devalues their otherwise valuable personal information. Although this damages theory has historically found little support from the courts, it's worth briefly mentioning in light of recent developments in the Ninth Circuit. The "reduced value" theory posits that personal information has its own independent value, and that disclosure of and potential widespread dissemination of the data in a breach deprives the plaintiff of that value. Thus far the theory has met with little success.

The *Barnes & Noble Pin Pad Litig.* Court captured the judiciary's cumulative attitude towards this theory succinctly: "The Plaintiffs' claim of injury in the form of deprivation of the value of their PII is insufficient to establish standing. Actual injury is not established under this

[25] *Id.* at *8 ("Neither is there any need to speculate as to whether the hackers intend to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so.").
[26] *Id.* at *9.

theory unless a plaintiff has the ability to sell his own information and a defendant sold the information."[27] There appears to be only one data breach case, *Claridge v. RockYou, Inc.,*[28] where this theory has been accepted.

RockYou, a social networking website, suffered a data breach in 2009 that affected approximately 32 million users.[29] Although users enjoyed RockYou's services free of charge, the plaintiff claimed that he suffered economic loss because he provided RockYou with his "PII, and that the PII constitutes valuable property that is exchanged not only for defendant's products and services, but also in exchange for defendant's promise to employ commercially reasonable methods to safeguard the PII that is exchanged. As a result, defendant's role in allegedly contributing to the breach of plaintiff's PII caused plaintiff to lose the 'value' of their PII, in the form of their breached personal data."[30]

Citing a scarcity of controlling legal authority on the matter, and the relative novelty of data breach cases at that time, the Court held that although it had doubts about "plaintiff's ultimate ability to prove his damages theory … [plaintiff's allegations of harm were sufficient] to allege a generalized injury in fact" at the motion to dismiss stage.[31] While no other court appears to have embraced the theory, the recent, unpublished Ninth Circuit decision in *In re Facebook Privacy Litig.*[32] may have given new life to the largely discarded theory that the mere loss of

---

[27] *See* In re Barnes & Noble Pin Pad Litigation, No. 12-cv-8617, 2013 WL 4759588 at *5 (N.D. Ill. Sept. 3, 2013) (citing cases); *see also* In re Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 442 (D. Del. 2013) ("the court concludes that . . . plaintiffs have not sufficiently alleged that the ability to monetize their PII has been diminished or lost by virtue of Google's previous collection of it"); In re DoubleClick, Inc. Privacy Litig., 154 F.Supp.2d 497, 525 (S.D.N.Y.2001) ("Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers. However, we are unaware of any court that has held the value of this collected information constitutes damage to consumers or unjust enrichment to collectors.").
[28] 785 F. Supp. 2d 855, (N.D. Cal. 2011).
[29] *Id*. at 858.
[30] *Id*. at 861.
[31] *Id*.
[32] 572 F. App'x. 494 (9th Cir. 2014).

control over valuable personal information is sufficient to constitute economic damage. The *In re Facebook Privacy Litig.* plaintiff had appealed the district court's dismissal of claims for breach of contract and violation of two California consumer fraud statutes (each of which required the "loss of money or property" to state a claim).[33] In a brief (and unpublished) opinion, the Ninth Circuit held that the plaintiff had sufficiently pled contract damages (but not the "loss of money or property" necessary for the consumer fraud claims) by alleging that "the information disclosed by Facebook can be used to obtain personal information about plaintiffs, and that they were harmed both by the dissemination of their personal information and by losing the sales value of that information."[34]

Going forward, it will be interesting to see whether this theory of harm makes a comeback. It is likely that, at least within the Ninth Circuit, practitioners will continue to test the theory—particularly with the emergence of marketplaces for consumers to directly sell access to their personal information.[35]

D. Misrepresentation / Overpayment.

Finally, a new damages theory that borrows principles from mislabeling and false advertising law has been making gains of late. In brief, the misrepresentation (also known as the "benefit of the bargain") theory argues that when a plaintiff relies on a defendant's misrepresentation about the security measures it uses to safeguard sensitive information, and a subsequent data breach provides evidence that those measures weren't implemented, then the plaintiff wouldn't have paid—or would have paid less—for the defendant's product or service; essentially, the consumer did not receive the benefit of the bargain from their transaction.

---

[33] *Id.*
[34] *Id.*
[35] In Svenson v. Google, Inc., No. 13-cv-04080, 2014 WL 3962820, at *5 (N.D. Cal. Aug. 12, 2014), the court dismissed plaintiffs claim based on the loss of economic value to her improperly disclosed PII precisely because she could not alleged that a market existed for the information in question.

The theory probably traces its data breach origins to the Eleventh Circuit's decision in *Resnick v. AvMed, Inc.*, where plaintiffs alleged that: (i) they had paid defendant health insurance premiums, (ii) a portion of those premiums was intended to pay for the administrative costs of data security, and (iii) the defendant allegedly did not meet its promise to secure their private information in accordance with the industry standards.[36] Addressing whether the plaintiff had plausibly alleged an entitlement to damages,[37] the Court upheld plaintiffs' allegation that they "conferred a monetary benefit on AvMed in the form of monthly premiums," that AvMed "appreciates or has knowledge of such benefit," that AvMed used the premiums to "pay for the administrative costs of data management and security," and that AvMed "should not be permitted to retain the money belonging to Plaintiffs ... because [AvMed] failed to implement the data management and security measures that are mandated by industry standards … as can be seen from the data breach."[38]

More recently, the plaintiff in *In re LinkedIn User Privacy Litig*. alleged that she viewed and read LinkedIn's privacy policy—which promised to use "industry standard" security measures—that she would not have paid for her premium subscription (even if it contained the same privacy promise as the free version of the service) but for that security promise, and that the promise ended up being false as evidenced by a 2012 data breach—i.e., the defendant had

---

[36] Resnick, 693 F.3d at 1322-24. While *Resnick* is often cited for its impact on standing doctrine, a careful reading of the Eleventh Circuit's decision belies this assertion. In its standing analysis, the Court found that plaintiffs had sufficiently stated an injury-in-fact where "they have become victims of identity theft and have suffered monetary damages as a result." *Id*. at 1324. In a subsequent decision out of an Eleventh Circuit district court, *Willingham v. Global Payments, Inc.*, No. 12-CV-01157, 2013 WL 440702, at *8 (N.D. Ga. Feb. 5, 2013), the court found no standing where the plaintiff failed to allege that fraudulent charges to her account were not reimbursed.

[37] While standing and damages are different inquiries, they do share some overlap. That is, any plaintiff who suffers damages has necessarily suffered the injury-in-fact required for standing. *See* Natural Res. Def. Council, Inc. v. U.S. Food & Drug Admin., 710 F.3d 71, 85 (2d Cir. 2013), as amended (Mar. 21, 2013) ("Even a small financial loss is an injury for purposes of Article III standing.") The opposite, of course, is not always true. *See Pisciotta*, 499 F.3d at 640.

[38] *Id*. at 1328.

allegedly not in fact been using industry-standard security.[39] The Court found these allegations sufficient to plead the injury-in-fact required by Article III and the economic harm required under California's Unfair Competition Law.[40] Relying on a series of Ninth Circuit cases involving state consumer protection claims for false labeling, the court found that because the plaintiff alleged that (1) she had purchased her premium subscription in reliance on LinkedIn's security standards statements, (2) these statements were false, and (3) that she wouldn't have purchased such the premium service but for the misrepresentation, the plaintiff had sufficiently alleged economic loss under the fraud prong of the California Unfair Competition Law ("CUCL"), and an injury-in-fact sufficient to confer Article III standing.[41]

Likewise, the *In re Adobe Sys., Inc. Priv. Litig.* Court heavily relied on California's numerous consumer protection laws in ruling that plaintiffs had statutory standing to sue under the CUCL, as Adobe had a duty to disclose that its security practices were not up to industry standards.[42] Plaintiffs positively identified a number of specific industry-standard security measures that Adobe allegedly did not implement, and further alleged that Adobe's competitors did invest in these measures. The court found that plaintiffs had therefore plausibly alleged—under the fraud and unfairness prongs of the CUCL—that Adobe gained an unfair competitive

[39] No. 5:12-cv-03088, 2014 WL 1323713, at *5 (N.D. Cal. Mar. 28, 2014).
[40] In a prior round of motion practice spurred by a LinkedIn Motion to Dismiss, the court had found that such a "benefit of the bargain" theory was not appropriate where the plaintiff did not allege that she had read and relied on LinkedIn's privacy representations in coming to her decision to purchase the LinkedIn premium service. *See* In re LinkedIn User Privacy Litigation, 932 F. Supp. 2d 1089, 1093-94 (N.D. Cal. 2013). Moreover, the court found that "in cases where the alleged wrong stems from allegations about insufficient performance or how a product functions . . . plaintiffs [must] allege 'something more' than 'overpaying for a 'defective product.'" *Id.* at 1094. Notably, in the briefing on the second motion to dismiss, plaintiff conceded, based on evidence provided by LinkedIn, that her claims for breach of contract and the unfair prong of the California Unfair Competition Law could not survive under her theory.
[41] *Id.*
[42] In re Adobe Sys., Inc. Priv. Litig., No. 13-cv-05226, 2014 WL 4379916, at *21 (internal citations omitted).

advantage by not spending money on security the way its competitors did.[43] Plaintiffs also plausibly alleged that their reliance on Adobe's alleged misrepresentations was sufficient to show injury in that they overpaid for Adobe products as a result.[44]

Courts have only recently begun to address the misrepresentation /overpayment theory of damages in data breach cases, making it difficult to divine whether this theory will continue to gain support. It warrants mentioning though that defendants in both *Resnick* and *In re LinkedIn User Privacy Litig*. agreed to settle rather than proceed to the discovery stage. These results will likely further encourage plaintiff's lawyers to pursue this line of argument where possible in data breach cases.

E. Shifting Trends

The ever-changing landscape of data breach litigation remains one of this rapidly developing field's defining characteristics. It has been a mere eleven years since California enacted the United States' first data security breach notification law, SB 1386.[45] Even the forward-thinking individuals behind that statute, however, likely did not anticipate the comprehensive shift towards big data and shared computing at the forefront of today's privacy and data security issues. Equally unlikely is that many people in 2003 believed that data breaches would emerge as the mid-2010s class action *cause célèbre*.

And although consumer plaintiffs have struggled to find a reliable route past motions to dismiss, creative litigators have experienced some success in satisfying Article III's standards.[46] At least a portion of this success is attributable to more careful adherence to the required

[43] *Id*. at *22.
[44] *Id*.
[45] Cal. Civ. Code §§ 1798.29; 1798.90 *et seq.*
[46] *See* Sec. II.E, *supra*.

pleading particularities of data breach cases that the courts have slowly outlined through their orders dismissing plaintiffs' cases (often times with leave to amend).[47]

As discussed above, the key to consistently sustaining viable causes of action will be a workable model of damages sufficient to satisfy Article III. While it remains to be seen whether courts are latching on to alternative standing theories in sufficient numbers to constitute a trend, there can be no doubt certain plaintiffs with fact-specific types of claims are surviving motions to dismiss. Until these theories percolate up through the circuit courts, as with *AvMed* in the Eleventh Circuit and *In re Facebook Privacy Litig.* in the Ninth, the exact boundaries of standing in data breach cases will remain imprecisely defined. Given the expense associated with defending these claims[48] and the resulting swiftness with which these lawsuits settle when plaintiffs do survive a motion to dismiss,[49] however, it may be that appellate guidance will take some time.

Nevertheless, there is a class of plaintiffs that avoids the litany of pleading frustrations faced by consumers—the financial institutions and other payment-card intermediaries which have traditionally absorbed the costs of fraudulent activity resulting from stolen PII. Indeed, the very condition that often dooms consumer claims—generally consumers affected by fraud are

---

[47] *Compare* In re LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089 (N.D. Cal. 2013) (dismissing claims where plaintiff failed to allege reliance on LinkedIn's privacy statements), *with* In re LinkedIn User Privacy Litig., No. 5:12-CV-03088-EJD, 2014 WL 1323713, at *8 (N.D. Cal. Mar. 28, 2014) (denying LinkedIn's motion to dismiss where plaintiff alleged that she read and relied on LinkedIn's privacy representations).

[48] A recent study by NetDiligence, a cyber-risk assessment firm, found the *average* cost for legal defense related to a data breach lawsuit was nearly $575,000. Mark Greisiger, *NetDiligence Cyber Liability & Data Breach Insurance Claims: A Study of Actual Claim Payouts*, NetDiligence.com (2013), http://www.netdiligence.com/files/CyberClaimsStudy-2013.pdf.

[49] *See, e.g.* In re Sony Gaming Networks & Customer Data Sec. Breach Litig., Order Granting Plaintiffs' Motion for Preliminary Approval of Class Action Settlement, No. 11-MD-2258 (MDD) (S.D. Cal. July 10, 2014) (granting preliminary approval of $15 million settlement (not including $2.75 million for attorneys' fees) following a January 2014 ruling leaving intact claims brought under consumer protection laws); Burrows v. Purchasing Power, LLC, Order Preliminarily Approving Class Action Settlement, No. 12-cv-22800, (S.D. Fla. April 12, 2013) (granting preliminary approval of a $430,000 settlement following the partial denial of Purchasing Power's motion to dismiss in early December 2012).

not liable to their bank or card provider for fraudulent claims on their accounts—provides the requisite injury-in-fact for a financial institution's claim against a breached entity to survive the pleading stage.[50] Because card issuers often use their authority under the Payment Card Industry Data Security Standards (PCI DSS) to fine non-PCI DSS complaint merchants and recover costs associated with a breach, however, lawsuits against breached merchants by the issuing banks have historically been rare.

Yet as breaches escalate in frequency, size, and cost, it is likely that more financial institutions will seek to recover their outlays from offending merchants. The infamous Target data breach, announced in December 2013 and affecting over 40 million card holders,[51] has spawned a number of class actions, including one comprised of affected financial institutions. A group of banks and credit unions have filed suit against the retailer for damages stemming from the record-setting breach.[52] Because of the relative dearth of case law regarding the duty of care owed by retailers to card issuers, it is likely that the Target class action will serve as a bellwether for other similar breaches.[53]

---

[50] In 2008, for example, credit card transaction vendor Heartland Payment Systems, Inc. suffered a breach affecting as many as 100 million cards issued by more than 650 financial services companies. Heartland would ultimately settle with Visa for nearly $60 million, MasterCard for $41.4 million, and with American Express for $3.6 million. *See* Tracy Kitten, *More Litigation Tied to Heartland Breach*, BankInfoSecurity.com (Feb. 21, 2013), http://www.bankinfosecurity.com/more-litigation-tied-to-heartland-breach-a-5528/op-1. Heartland continues to litigate claims levied by a number of card issuing banks. *See* Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013).

[51] *The Target Breach, By the Numbers*, Krebs on Security.com (May 6, 2014), http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers.

[52] In re Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522 (PAM/JJK) (D. Minn.).

[53] Of particular note is the recent payment card breach involving Home Depot, which affected nearly 56 million payment cards over a five-month span. On September 16, 2014, Home Depot was sued as part of a proposed class action in the Northern District of Georgia. *See* First Choice Federal Credit Union v. The Home Depot, Inc., No. 1:14-cv-2975-AT (N.D. Ga. 2014). Plaintiff First Choice Federal Credit Union seeks to represent a class of credit unions, banks, and other financial institutions affected by the payment card system breach.

One area where consumer plaintiffs have been able to avoid the standing pitfalls is in suing under privacy-related laws that provide for statutory damages without proof of actual monetary harm.[54] Several courts have held that financial harm is not required under such laws, so long as the plaintiff successfully pleads the impairment of her statutory rights.[55]

The defense bar, however, has made a concerted effort to challenge this vision of the standing doctrine, and the Supreme Court's upcoming decision on the petition for *certiorari* in *Spokeo, Inc. v. Robins*, a case involving standing and the statutory damages provision of the Fair Credit Reporting Act, may provide further insight. Defendants contend that the *Spokeo* petition will determine whether Congress can confer Article III standing upon a plaintiff who suffers no concrete harm by authorizing a private right of action based on a bare violation of a federal statute.[56] The plaintiffs' bar views the *Spokeo* question differently, and instead believes that the Court will be asked whether or not to uphold its long-standing precedent that "[t]he injury required by Article III can exist solely by virtue of statutes creating legal rights, the invasion of which creates standing."[57]

---

[54] While no state data breach notification laws yet provide for statutory damages, there are a number of state and federal consumer protection laws that do, such as the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, and the Fair and Accurate Credit Transactions Act, 15 U.S.C. §§ 1681c(g), 1681n.

[55] *See, e.g.* Sterk v. Redbox Automated Retail, LLC, No. 13-3037, 2014 WL 5369416, at *3 (7th Cir. Oct. 23, 2014) ("As we have said, Congress 'may not lower the threshold for standing below the minimum requirements imposed by the Constitution,' but Congress does have the power to 'enact statutes creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute.'") (quoting Kyles v. J.K. Guardian Sec. Servs., Inc., 222 F.3d 289, 294 (7th Cir. 2000)); In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1055 (N.D. Cal. 2012) (Koh, J.) (finding that allegations that mobile industry defendants violated plaintiffs' statutory rights under the Stored Communications Act sufficiently established an injury-in-fact for purposes of Article III standing).

[56] Petition for a Writ of Certiorari at 1, Spokeo, Inc. v. Robins, (No. 13-1339), 2014 WL 1802228.

[57] *See* Warth v. Seldin, 422 U.S. 490, 500 (1975); *see also* Antonin Scalia, *The Doctrine of Standing as an Essential Element for the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 885 (1983) ("Standing requires . . . the allegation of some particularized injury to the individual plaintiff. But legal injury is by definition no more than the violation of a legal right; and legal rights can be created by the legislature.").

The resolution of the *Spokeo* petition will likely impact the next wave of state data breach notification laws by determining whether or not the evolution of consumer privacy laws will include statutory damages provisions within—and accordingly opening the doors of federal court to the aggrieved consumer.[58]

Finally, recent lawsuits have shown that the defense bar's Article III standing offensive may have unintended consequences, as recent cases have shown that data-breach class-action plaintiffs may progress further by simply side-stepping Article III standing issues and filing their lawsuits in state courts. State courts are not bound to the Article III standing doctrine fashioned by the federal courts, and are perceived as having less severe—or at least less technical—requirements in order to assert standing to bring a lawsuit.[59] And while class-action plaintiffs may have trouble keeping their lawsuits in state courts in the first instance—as the Class Action Fairness Act (CAFA)[60] sets limits on the amount in controversy and diversity of class membership that may be heard in state court[61]—those cases will only end up remanded to state court if the federal courts lack Article III jurisdiction to hear the claims.[62] Furthermore, non-CAFA plaintiffs have found recent success in state courts with damages theories that have

---

[58] Several states already maintain a private right of action through their breach notification statutes, including California, Massachusetts, and New Hampshire.

[59] William A. Fletcher, *The "Case or Controversy" Requirement in State Court Adjudication of Federal Questions*, 78 CALIF. L. REV. 263, 264-65 (1990); *see also* James W. Dogget, *"Trickle Down" Constitutional Interpretation: Should Federal Limits on Legislative Conferral of Standing Be Imported Into State Constitutional Law?*, 108 COLUM L. REV. 839, 851 (2008) ("Since state courts are not organized under the Federal Constitution, but rather under state constitutions, states have been free to vary justiciability standards in their courts from federal norms.).

[60] 28 U.S.C. §§ 1332(d), 1453, 1711-1715.

[61] Under CAFA, federal courts are granted jurisdiction over certain class actions in which the amount in controversy exceeds $5 million and any class members are citizens of a state different from any defendant. This diversity limitation may be overcome, however, if at least two-thirds of the class members and the "primary" defendant are citizens of the state in which the action was originally filed. Plaintiffs cannot overcome the amount in controversy requirement merely by stipulating that the damages sought are less than $5 million. *See* Standard Fire Ins. Co. v. Knowles, 133 S. Ct. 1345, 1349-50 (2013).

[62] *See* 28 U.S.C. § 1147 ("[I]f at any point before final judgment it appears that the district court lacks subject matter jurisdiction, the case shall be remanded.").

largely failed in the federal courts.[63] If additional state courts show a willingness to entertain previously challenged damage theories, it is possible that while defendants have traditionally sought to avoid state courts at all costs, much of what is now federal litigation would migrate to friendlier state courts.

Finally, some plaintiffs believe that the proliferation of arbitration agreements in consumer contracts of adhesion may offer an additional avenue for seeking redress. They argue that, as a creature of contract law, an arbitrator's jurisdiction is not limited by Article III's injury-in-fact requirement. Thus, plaintiffs argue, they may be permitted to bring class arbitrations or hundreds of individual arbitrations under the appropriate circumstances.

III. CONCLUSION

Data breach plaintiffs have been waging an uphill battle to have their claims heard. While plaintiffs allege that the personal information at the heart of data breaches clearly has some inherent value—why else would companies value it and legislatures protect it, they contend—the federal courts have been generally resistant to lawsuits that fail to allege actual financial injury. Plaintiffs continue to develop new theories, often borrowed from other areas of the law, under which to plead these claims. As some recent cases have shown, the federal courts may finally be relaxing the Article III barrier. Regardless, as the incidence of data breaches continues to climb at a near exponential pace, there is no doubt that affected consumers and institutions will seek attempt to seek redress through the courts, and their characterizations of cognizable injury will continue to evolve.

---

[63] *See* Tabata v. Charleston Area Med. Ctr., Inc., 759 S.E. 2d 459. In *Tabata*, the West Virginia Supreme Court found that hospital patients had a "concrete, particularized, and actual" interest "in having their medical information kept confidential." *Id.* at 464. Plaintiffs had not alleged any financial harm or even that their patient data had been improperly accessed. It remains to be seen whether *Tabata* will be applied to cases outside of West Virginia or that do not involve medical information.