White Paper

Consumer Class Actions Arising from Data Breaches Present a Battleground for Standing to Bring Suit

VORYS

Higher standards make better lawyers.®

By: Eric W. Richardson, Nathan L. Colvin and Timothy C. Dougherty
A version of this article will appear in an upcoming volume of The Northern Kentucky Law Review.

Announcements of data breaches quickly turn the gears of the court system, as class action attorneys waste little time in acting upon the potential large-scale liability from such breaches. When Target announced in December 2013 that it had suffered a data breach that potentially exposed information for forty million customers, fifteen class action lawsuits were filed against the company within a week.[1] This comes as no surprise when the damages from a class action suit can stretch over the hundred-million-dollar mark and the average attorney fees for data breach litigation is more than one million dollars.[2] Of course, class action plaintiffs' counsel want to establish position to control major litigation that is a prime candidate for expansion into even larger multidistrict litigation. But in many cases, plaintiffs' counsel may be acting too quickly by filing before identifying a putative class representative with an injury sufficient to establish standing and invoke the court's jurisdiction.

Standing Requirements Restrict Lawsuits to Claims Alleging Actual Injury

Consumer class actions arising out of data breaches arise under numerous theories of liability, ranging from negligence, breach of fiduciary duty, and breach of implied contract to invasion of privacy and state and federal statutory violations such as the Fair Credit Reporting Act, 15 U.S.C. § 1281 *et seq*. But regardless of the claims, all plaintiffs must establish standing to get into federal court. To establish standing to maintain a lawsuit in federal court under Article III of the United States Constitution, an injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[3]

Thus, a plaintiff must have suffered an actual or imminent injury that the litigation can recompense. These requirements are established to ensure the judicial branch does not usurp the policymaking roles of the political branches.[4] For harm to qualify as imminent, the "threatened injury must be *certainly impending*."[5] Harm that is merely possible or speculative is not sufficient to invoke the jurisdiction of the federal courts,

---

[1] *Lawsuits against Target piling up*, CBS/Wire Services, Dec. 24, 2013, available at http://www.cbsnews.com/news/lawsuits-against-target-piling-up/.

[2] The Target breach led to settlements with banks for $39 million, customers for $10 million, and Visa for $67 million. Ahiza Garcia, *Target settles for $39 million over data breach*, CNN Money, Dec. 2, 2015, available at http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/. As of 2012, the average attorney fee recovery for data breach litigation was calculated at $1.2 million. *See* Sasha Romanosky et al., *Empirical Analysis of Data Breach Litigation*, Temple Univ. Beasley School of Law, Legal Studies Research Paper No. 2012-29 (2012) at 25. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461.

[3] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (quoting *Monsanto Co. v. Geertson Seed Farms*, 130 S. Ct. 2743, 2752 (2010)).

[4] *Clapper*, 133 S. Ct. at 1146 (emphasis added).

[5] *Id.* at 1147 (emphasis in original).

and state courts largely follow these same rules.[6] Data breach cases have frequently tested this requirement.

Factual Hurdles to Clear to Show Standing in Data Breach Claims[7]

Unless an action is brought pursuant to a statute that specifies the kind of injury sufficient to give rise to a suit,[8] for plaintiffs to show actual injury in data breach cases, they typically will need to clear two important hurdles. First, plaintiffs must show that their data was actually accessed in a meaningful way by hackers. In other words, plaintiffs must show that their data was personally identifiable information and that it was actually exfiltrated by the hackers. Did the hackers just hack into the system or did they actually exfiltrate information? Was the data personal information of such a nature that a group of plaintiffs could be harmed if that information was actually used? Was the data encrypted to a degree that it would be useless to hackers regardless of the underlying data contents? Although someone may not want a hacker to have one's name, showing harm from that information alone is more difficult than showing harm from the theft of one's name and a Social Security number or a credit card number. And even the most sensitive personal information may not give rise to harm if there is little reason to think the thief will be able to do anything with the information. If the plaintiffs' data was encrypted, or was never exfiltrated by the hacker, then the data may not have been accessed in a meaningful way by hackers.

Second, assuming that the plaintiffs can show that their stolen personal information was accessed in a meaningful way, the plaintiffs must then demonstrate that their data was actually misused by hackers or is in imminent danger of being misused. Because class action suits are frequently filed before the named plaintiff has any evidence of actual misuse of their data, both circuit and district courts around the country have struggled with how to apply traditional standing rules to a threat of potential misuse of personal data.

---

[6] *See, e.g., Cleveland v. Shaker Hts.*, 30 Ohio St.3d 49, 51, 507 N.E.2d 323 (1987) ("[T]he question of standing depends on whether the party has alleged. . . a personal stake in the outcome of the controversy.") (internal quotation marks omitted); *Kincaid v. Erie Ins. Co.*, 128 Ohio St.3d 322, 2010-Ohio-6036, 944 N.E.2d 207, ¶ 13 (finding no justiciability where plaintiff had not yet suffered loss).

[7] In May 2016, the Supreme Court rendered its decision in Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 194 L. Ed. 2d 635 (2016), in which the Court considered and rejected the contention that, where the plaintiff has not otherwise suffered a concrete and particularized injury, Congress can bestow Article III standing on a plaintiff to bring an action based on a violation of a statute. Although many hoped that the decision would clarify more broadly the injury-in-fact requirement for standing in data breach cases, the *Spokeo* decision offered little additional guidance and has been interpreted as merely reiterating traditional standing principles. *See In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, No. 15-2309, 2017 WL 242554, at *9–10 (3d Cir. Jan. 20, 2017) ("[W]e do not believe that the [*Spokeo*] Court so intended to change the traditional standard for the establishment of standing…. *Spokeo* itself does not state that it is redefining the injury-in-fact requirement…. In the absence of any indication to the contrary, we understand that the *Spokeo* Court meant to reiterate traditional notions of standing….").

[8] As explained above, most data breach class actions allege common law tort or contract claims. But in some instances, class actions plaintiffs have brought statutory claims based on statutes that specify a lower threshold of injury that is sufficient to bring suit. *See, e.g., Matera v. Google Inc.*, No. 15-cv-04062, 2016 U.S. Dist. LEXIS 130778, *41 (N.D. Calif. Sept. 23, 2016) (holding that invasion of privacy is injury sufficient to grant standing pursuant to the Wiretap Act 18 U.S.C. § 2511(a)(1) and the California Invasion of Privacy Act, Cal. Penal Code § 631).

Actual Misuse of Data Satisfies Requisite Harm

As an initial matter, courts uniformly have found that actual misuse of a plaintiff's personally identifiable information is sufficient to establish standing. Where plaintiffs can show that the theft of their information has led to identity theft, new lines of credit being taken in the plaintiffs' names, injury to their credit rating and the like, courts have found that actual harm has been incurred and, thus, the requirements of standing have been satisfied. For example, in *Lambert v. Hartman*, the Sixth Circuit held that a plaintiff had adequately established the requirements of standing where the plaintiff demonstrated that the hacker's theft and misuse of her personal information had injured her credit rating.[9] In *Resnick v. AvMed, Inc.*, the Eleventh Circuit similarly found that the plaintiff had established standing where the hacker's theft of unsecured laptops had led to unauthorized lines of credit being opened in the plaintiffs' names.[10]

Courts Struggle with Drawing the Line for Standing in Data Breaches

While courts had no trouble finding standing where there was an allegation of actual misuse of personally identifiable information, the first courts to deal with class actions that lacked such allegations split on the question of standing.

The majority of courts first addressing this question found standing where plaintiffs had merely alleged an increased risk of harm. For example, in *Pisciotta v. Old National Bancorp*, the Seventh Circuit held that standing was established in a data breach where the plaintiffs spent resources on credit monitoring and suffered an "increas[ed] risk of future harm."[11] Further, in *Krottner v. Starbucks Corp.*, the Ninth Circuit held that the risk of harm posed by the theft of a laptop with unencrypted names, addresses, and Social Security numbers posed a "credible threat of harm" that was "real and immediate, not conjectural or hypothetical," even though no actual misuse had occurred by the time of the lawsuit.[12] Indeed, some courts even held that "the fear or anxiety of future harm" – even in the absence of any actual harm – is a sufficiently cognizable injury to establish standing.[13] And other courts analogized data breaches to toxic tort cases, where no actual harm has been suffered yet, but

---

[9] *Lambert v. Hartman*, 5197 F.3d 433, 437 (6th Cir. 2006) (holding that the plaintiff had established standing where plaintiff "alleged that her identity was stolen and that her financial security and credit rating suffered as a result.").

[10] *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1322, 1329-30 (11th Cir. 2012) ("Plaintiffs allege that they have become victims of identity theft and have suffered monetary damages as a result. This constitutes injury in fact under the law."); *Curry v. AvMed, Inc.*, No. 10-cv-24513, 2014 U.S. Dist. LEXIS 48485, *2-3 (S.D. Fla. Feb. 28, 2014).

[11] *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 632, 634 (7th Cir. 2007) (standing satisfied by "increas[ed] risk of future harm").

[12] *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141-43 (9th Cir. 2010) (finding credible threat of immediate harm when a laptop with personally identifiable information was stolen).

[13] *McLoughlin v. People's United Bank, Inc.*, No. 3:08-cv-00944, 2009 U.S. Dist. LEXIS 78065, *11 (D. Conn. Aug. 31, 2009) (standing based on "the fear or anxiety of future harm"); *see also Krottner*, 628 F.3d at 1141-42.

the court presumes that an injury will occur in the future due to the plaintiff's "exposure."[14]

Nonetheless, not all courts have allowed a plaintiff to proceed merely on a showing of an increased risk of harm. In fact, a minority of courts has refused to find standing without an allegation of actual harm or actual misuse of a plaintiff's personally identifiable information. In the seminal minority position case, *Reilly v. Ceridian Corp.*, the Third Circuit Court of Appeals considered a data breach where a hacker had infiltrated a company's security, but the plaintiff could not show that the hacker had actually read, copied or understood the personal information, nor that the hacker intended or was capable of criminal misuse.[15] Under those circumstances, the Third Circuit concluded that the plaintiffs failed to establish standing because the potential harm was "neither imminent nor certainly impending,"[16] and it rejected the proposition that increased risk alone is sufficient to establish standing.[17] Further, even though the plaintiffs had paid for credit monitoring services in the wake of the data breach, the court held that such costs were voluntarily undertaken in the absence of an imminent harm and, thus, plaintiffs' choice to pay these costs could not establish actual harm to the plaintiffs.[18]

Clapper Reinforces Standing Bar Against Conjectural Harm, Albeit in a Different Context

The United States Supreme Court has not yet addressed the question of standing in a data breach context. But in 2013, in *Clapper v. Amnesty International*, the Supreme Court issued a critical Article III standing decision dealing with the absence of a showing of actual harm that has greatly impacted the way lower courts have addressed standing in data breach class actions.[19]

Specifically, the *Clapper* Court considered a challenge by Amnesty International and others as to the constitutionality of the Foreign Intelligence Surveillance Act, through which the Attorney General and the Director of National Intelligence were authorized to obtain approval from the Foreign Intelligence Surveillance Court to conduct surveillance on individuals who are not "United States persons" and who are reasonably believed to be located outside of the United States.[20] Notably, such

---

[14] *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 280 (S.D.N.Y. 2008) (standing for class of 300,000, analogizing a data breach to an exposure to toxic chemicals).

[15] *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011).

[16] *Id.*

[17] *Id.* at 43.

[18] *Id.* at 46; *see also Willingham v. Global Payments, Inc.*, No. 1:12-cv-01157, 2013 U.S. Dist. LEXIS 27764, *20 (N.D. Ga. Feb. 5, 2013).

[19] *Clapper v. Amnesty Int'l*, 133 S. Ct. 1138 (2013).

[20] 133 S. Ct. at 1140.

surveillance could be authorized without a showing of probable cause to believe that the target of the surveillance was, in fact, an agent of a foreign power.[21]

In that case, the plaintiffs alleged that there was an objectively reasonable likelihood that the communications of Amnesty International's employees – who are United States residents who regularly communicate during the course of their employment with the potential targets of the statute – would be intercepted pursuant to the statute.[22] The plaintiffs also alleged that the risk of surveillance under the statute was so substantial that they had to take costly measures to secure their communications.[23]

Notwithstanding the expressed concerns, the Supreme Court rejected the plaintiffs' arguments and held that they had failed to demonstrate actual or imminent harm sufficient to establish standing. The Supreme Court held that the plaintiffs' theory of standing required speculation that Government actors would actually target plaintiffs' communications; that they would do so via the statutory authorization instead of a traditional warrant; and that the Government would successfully acquire the communications.[24] The Court also rejected the claim that plaintiffs had already suffered harm by taking security precautions fairly traceable to the statute because precautions taken without an imminent threat of harm are not fairly traceable.[25] In short, the Supreme Court held that a plaintiff's "subjective fear of surveillance does not give rise to standing."[26]

Inconsistent Attempts by Courts to Apply *Clapper* to Data Breach Cases

In the aftermath of *Clapper*, district courts were initially "more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases."[27] Rather than a "credible threat" of harm, those courts required a more exacting factual basis before finding an imminent threat of injury.

For example, the District Court for the District of Columbia found no imminent threat of injury where a car theft resulted in the loss of backup tapes with names, Social Security numbers, dates of birth, and medical information (but not bank or credit card information), because those tapes required specific hardware and software to understand and use.[28] Similarly, an online breach of personally identifiable

---

[21] *Id.* at 1144.

[22] *Id.* at 1146.

[23] *Id.*

[24] *Id.* at 1147-48.

[25] *Id.* at 1151.

[26] *Id.* at 1152-53.

[27] *In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 28 (D.D.C. 2014).

[28] *Id.* at 20.

information from eBay accounts (but not bank or credit information, nor Social Security numbers) did not demonstrate an imminent threat of injury because there had no allegation of misuse (or attempted misuse) of the information.[29] And earlier this year, the District Court of Minnesota found no standing where plaintiffs alleged a data breach involving malicious software installation to the portion of a network that processed credit card payments—even when one plaintiff faced a fraudulent charge on his credit card—because (i) none of the other sixteen plaintiffs faced similar actions and (ii) the lone plaintiff affected did not allege ultimate monetary loss because he immediately cancelled his credit card.[30]

Matters were looking so bleak for class action plaintiffs that some enterprising attorneys began to allege that the plaintiffs were injured because their personally identifiable information was less valuable on the black market as a result of a data breach. In the district court proceedings in *Galaria v. Nationwide Mutual Insurance Co.*, for example, plaintiffs alleged that there is a "cyber black market" in which they could sell personal information for profit and that the hacking deprived them of that value.[31] Not surprisingly, the district court found that plaintiffs had not sufficiently alleged how they had been deprived of the value of their personal information by being deprived of the opportunity to sell that information on the black market.[32]

Despite this initial trend towards more rigorous standing in the immediate aftermath of *Clapper*, the courts of appeals have begun to swing back to the pre-*Clapper* view of standing in data breach cases. In *Galaria*, for example, the Sixth Circuit reversed the district court and concluded the plaintiffs had standing, noting that there was a "sufficiently substantial risk of harm" and that it would be "unreasonable to expect Plaintiffs to wait for actual misuse" of their personally identifiable information before bringing suit.[33] Continuing, the Sixth Circuit noted that, as a result of the hack, the plaintiffs' information was possessed by criminals and, thus, that harm to the plaintiffs was likely to be imminent—reasoning that would appear to apply to virtually all hacking and other theft cases.[34] (The Sixth Circuit did not address plaintiffs' argument that, as a result of the hack, their personally identifiable information was less valuable and that the plaintiffs would be unable to sell their own information for as much as they might otherwise have.)

Similarly, courts in the Seventh and Ninth Circuits have concluded that *Clapper* did not disturb the pre-*Clapper* decisions in *Pisciotta* and *Krottner*. In *Remijas v. Neiman Marcus Group, LLC,* the Seventh Circuit distinguished *Clapper* by noting that,

---

[29] *Green v. eBay Inc.*, No. 14-1688, 2015 U.S. Dist. LEXIS 58047, *20 (E.D. La. May 4, 2015).

[30] *In re SuperValu, Inc.*, No. 14-MD-2586, 2016 U.S. Dist. LEXIS 2592, *4-6, 20 (D. Minn. Jan. 7, 2016).

[31] *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 658-59 (2013).

[32] 998 F.Supp. 2d at 659-60.

[33] *Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 U.S. App. LEXIS 16840, *10 (6th Cir. Sept. 12, 2016).

[34] 2016 U.S. App. LEXIS 16840 *9-10.

whereas there was no evidence that any plaintiffs were monitored by the Government in *Clapper*, the credit card information of the plaintiffs in the case at bar was known to be stolen and, further, around three percent of the accounts had been the target of fraudulent activity.[35] Thus, the Seventh Circuit held that there was an "objectively reasonable likelihood" that the plaintiffs would suffer injury in the future and that such a prospect established standing, despite the Supreme Court's seeming rejection of that standard under the *Clapper* facts. Similarly, in *Corona v. Sony Pictures Entertainment, Inc.*, the Central District of California found that *Krottner*'s "credible threat of real and immediate harm" standard survives *Clapper* despite differences in language.[36] In *Corona*, the court found real and immediate risk of harm where plaintiffs alleged that personal information was stolen and posted on a file-sharing website for identity thieves to access and where some plaintiffs had received threats of harm to its employees.[37]

The Next Hurdle on the Horizon: Harm Sufficient to State a Claim

The most recent trend of appeals courts distinguishing *Clapper* in data breach class actions could prove to be temporary, as courts turn their attention to whether the plaintiffs have pleaded actionable harm sufficient to state a claim for relief. Although this difference was noted by courts prior to *Clapper*, the hurdle was clearly demonstrated by a recent district court case that followed the Seventh Circuit's post-*Clapper* standing decision. In *In re Barnes & Noble Pin Pad Litigation* (N.D. Ill. Oct. 3, 2016), the court found a "substantial risk" of harm to plaintiffs sufficient to satisfy standing where the plaintiffs were Barnes & Noble customers who made purchases during a period in which skimmers stole data from store pin pad terminals and were alleged to have used such data for unauthorized purchases.[38] However, because no actual out-of-pocket loss was alleged, the court found that, although plaintiffs had standing to bring suit, they failed to allege damages sufficient to plead their causes of action, resulting in dismissal of their claims.[39]

Conclusion

More courts will undoubtedly continue to struggle with applying the Supreme Court's *Clapper* decision in the data breach context and to draw the line for the standing of class action plaintiffs. But even if the battleground ultimately moves from the issue of standing – as more courts adopt the lesser threshold recently articulated by the Sixth and Seventh Circuits – plaintiffs will likely be challenged if they cannot allege sufficient damages in support of their causes of action. And whether such hurdles begin to curtail consumer class actions has yet to be determined.

About the Authors:

[35] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693 (7th Cir. 2013).

[36] *Corona v. Sony Pictures Entmt, Inc.*, No. 14-cv-09600, 2015 U.S. Dist. LEXIS 85865, *5 (C.D. Calif. June 15, 2015).

[37] 2015 U.S. Dist. LEXIS 85865 at *5-6.

[38] *In re Barnes & Noble Pin Pad Litig.* No. 12-cv-08617, 2016 U.S. Dist. LEXIS 137078, *10-11 (N.D. Ill. Oct. 3, 2016).

[39] *E.g., id.* at *15-16, 24-25.

Eric W. Richardson is a partner in the Vorys Cincinnati office and a member of the litigation practice group. His practice is focused on civil litigation and white collar criminal defense work and encompasses complex commercial, banking, insurance, data breach, construction, and intellectual property litigation. Eric teaches information privacy and data protection law, and intellectual property law -- including patent, copyright and trademark law -- as an adjunct professor at the Northern Kentucky University – Salmon P. Chase College of Law.

Nathan L. Colvin is an associate in the Vorys Cincinnati office and a member of the litigation group. His practice is focused on complex civil litigation. Nathan also has experience with data security issues, including counseling clients that have suffered a data breach and working with clients to plan and prepare for a potential data breach. He received his J.D. *magna cum laude* from The Ohio State University Moritz College of Law, where he was a member of the Order of the Coif, the *Ohio State Law Journal* and moot court. He received his B.A. *cum laude* from Miami University.

Timothy C. Dougherty is an associate in the litigation group in the Vorys Cincinnati office. He received his J.D. from Vanderbilt University Law School, where he was a notes editor of the *Vanderbilt Law Review* and a student adviser for the National Moot Court Team. He received his B.A. *cum laude* from the University of Notre Dame.

This white paper is for general information purposes and should not be regarded as legal advice. Please contact the authors if you want more information or have questions about how these developments apply to your situation.