RISKY BUSINESS: WHETHER AN INCREASED RISK OF HARM SUPPORTS LEGAL STANDING IN DATA BREACH CLASS ACTIONS CONTINUES TO DIVIDE FEDERAL COURTS OF APPEALS

Date: 26 March 2018

U.S. Financial Institutions and Services Litigation / Class Action Litigation Defense Alert

By: Andrew C. Glass, David Christensen, Matthew N. Lowe

Every data breach class action in federal court must confront a threshold question: has the plaintiff alleged a sufficient "injury in fact" to establish Article III standing? The inquiry frequently focuses on whether a plaintiff has standing simply by pleading an increased risk of future injury from the theft of personal identifying information (PII). This is because many named plaintiffs do not—because they cannot—allege any present harm. The federal courts of appeals continue to weigh in on the issue of whether allegations of possible future harm suffice for Article III purposes. But far from providing clarity or consensus, recent appellate decisions have reached differing conclusions, which appear highly dependent on the nature of the facts alleged in each case. [1]

U.S. SUPREME COURT CLARIFIES REQUIREMENT FOR ESTABLISHING ARTICLE III STANDING BASED ON RISK OF FUTURE INJURY

Article III standing is a prerequisite to sustaining an action in federal court and requires plaintiffs to allege, and subsequently prove, that they have suffered an injury that is (1) "concrete, particularized, and actual or imminent," (2) "fairly traceable to the challenged action," and (3) "redressable by a favorable ruling." [2]

In *Clapper v. Amnesty International USA*, the Supreme Court addressed the question of when allegations of future injuries suffice for Article III standing purposes. [3] The Court held that a threatened injury must be "certainly impending" to create standing. The Court also noted that "[i]n some instances, [the Court has] found standing based on a substantial risk that the [future] harm will occur." [4] The *Clapper* Court held, however, that a theory of future injury fails either test when it "relies on a highly attenuated chain of possibilities." [5] And the Court expressly rejected a more lenient Article III standard proposed by the plaintiffs, which would have allowed for standing based upon an "objectively reasonable likelihood" of future injury. [6]

In *Spokeo, Inc. v. Robins*, [7] the Supreme Court again clarified the Article III standing requirements but did not specifically address future injuries. In *Spokeo*, the Court reemphasized that an injury must be both "concrete" *and* "particularized" to create standing and that the "concreteness" element requires that an injury "actually exist" for there to be standing. [8]

RECENT DECISIONS BY THE SIXTH, SEVENTH, NINTH, AND D.C. CIRCUITS

On one side of the ledger, the Sixth, Seventh, Ninth, and D.C. Circuits have found that under certain circumstances, plaintiffs can establish Article III standing based solely on an increased risk of future injury stemming from a data breach. [9] These decisions largely focus on whether the type of data stolen would permit hackers to commit identity theft.

Indeed, in the *Zappos.com, Inc.* data breach litigation, [10] the Ninth Circuit recently held that the plaintiffs had "sufficiently alleged an injury in fact based on a substantial risk that the Zappos hackers will commit identify fraud or identity theft" using the plaintiffs' stolen PII. [11] The Ninth Circuit explained that "the information [alleged to have been] taken in the data breach [] gave hackers the means to commit fraud or identity theft" because the data included the plaintiffs' names, account numbers, passwords, email addresses, mailing addresses, telephone numbers, and credit card numbers. [12] In response to the defendant's argument that the lack of any risk of injury was evident from the plaintiffs' failure to allege any actual injury in the six years that lapsed between the alleged data breach and the court's decision, the *Zappos* court disagreed and concluded that standing "depends upon the state of things at the time [an] action [is] brought." [13]

The D.C. Circuit examined similar allegations in *Attias v. CareFirst, Inc.* [14] There, the plaintiffs alleged that hackers had obtained their social security numbers, credit card numbers, names, birth dates, email addresses, and healthcare subscriber numbers as a result of a data breach. [15] The court held that these allegations were sufficient to establish standing—even without allegations of actual identify theft or fraud—because it was reasonable to infer that "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken." [16]

In *Galaria v. Nationwide Mutual Insurance Co.*, [17] the Sixth Circuit reached a similar decision, finding standing based on the increased risk of identity theft after a hacker breached the defendant's computer systems and stole PII, including names, dates of birth, social security numbers, and driver's license numbers. [18] The court noted that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for [] fraudulent purposes…" [19] Additionally, the Sixth Circuit gave weight to the fact that the defendant had offered free credit monitoring services to all those affected by the hack, noting that by doing so, the defendant "seems to recognize the severity of the risk" of misuse of the data. [20]

RECENT DECISIONS BY THE SECOND, FOURTH, AND EIGHTH CIRCUITS

On the other side of the ledger, the Second, Fourth, and Eighth Circuit have expressed reluctance to embrace theories of standing in data breach cases based solely on allegations of an increased risk of future injury. [21]

Most recently, in the *SuperValu, Inc.* data breach litigation, [22] the plaintiffs alleged that hackers stole their names, debit and/or credit card account numbers, expiration dates, card verification value codes (CVV), and associated PINs. The Eighth Circuit held, however, that such allegations were not sufficient to establish Article III standing. [23] Specifically, the court found the allegedly stolen data was not of a type that generally could be used to open unauthorized accounts in the plaintiffs' names, "which is 'the type of identity theft generally considered to have a more harmful direct effect on consumers.'" [24] The court also noted that a study and report by the U.S. Government Accountability Office (GAO) had found that "most [data] breaches have not resulted in detected incidents of identity theft." [25] The Eighth Circuit also did not credit the plaintiffs' allegations that the data was being sold by third-parties on "illicit websites." [26] The court disregarded such allegations because they did not indicate any actual harm to the plaintiffs themselves. [27]

In *Whalen v. Michaels Stores, Inc.*, [28] the Second Circuit rejected the plaintiff's standing theory, finding that the allegedly hacked information was limited in scope. Specifically, the plaintiff had alleged that she had standing as a result of the increased "risk of future identity fraud" stemming from a breach that exposed her credit card number and expiration date. [29] The Second Circuit rejected this theory, stating that the plaintiff "does not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen." [30]

The Fourth Circuit reached a similar result. In *Beck v. McDonald*, [31] the plaintiffs brought suit alleging that a laptop and boxes of documents containing PII—including names, social security numbers, and medical information—had been lost or stolen from a Veterans Affairs medical center. [32]The Fourth Circuit rejected the plaintiffs' assertion of standing, because it relied on an "attenuated chain of possibilities." In particular, the court found that the plaintiffs had not alleged that "the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information." [33] Unlike the Ninth Circuit in the *Zappos* decision discussed above, the Fourth Circuit indicated that standing is affected by the passage of time. The court held that "'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative." [34] The Fourth Circuit also rejected the plaintiffs' argument that the defendant had admitted the risk of identity theft was great by offering free identity protection services and noted that "such a presumption would surely discourage organizations from offering these services to affected individuals." [35]

SUPREME COURT DECLINES TO ENTER THE FRAY – FOR NOW

Despite the apparent circuit split in how strictly or liberally to interpret the question of future injury in the context of data breach litigation, the U.S. Supreme Court recently declined the opportunity to address the issue. Specifically, the defendant in the *Attias v. CareFirst, Inc.* decision filed a petition for a writ of certiorari, presenting the question of "[w]hether a plaintiff has Article III standing based on a substantial risk of harm that is not imminent and where the alleged future harm requires speculation about the choices of third-party actors not before the Court." [36] On February 20, 2018, the Supreme Court denied the petition. [37]

Accordingly, the circuit courts may well continue to arrive at different conclusions as to whether the circumstances surrounding a data breach present a substantial risk of harm to consumers. We will continue to monitor and report on developments in data breach standing law as they unfold.

---

[1] For a summary of how courts have treated other standing theories advanced by class plaintiffs in data breach class actions, especially the "benefit of the bargain" theory of standing, see our article at http://www.klgates.com/hold-on-you-didnt-overpay-for-that--courts-address-new-overpayment-theory-from-plaintiffs-in-data-breach-cases-08-10-2016/.

[2] *See*, *e.g.*, *Spokeo, Inc. v. Robins*, 578 U.S. ----, 136 S. Ct. 1540, 1547 (2016); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)); *see also Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180–81 (2000).

[3] 568 U.S. 398 (2013).

[4] *Id.* at 409–10, 414 n.5.

[5] *Id.* at 409–10.

[6] *Id.* at 410.

[7] 578 U.S. ----, 136 S. Ct. 1540 (2016).

[8] *Id.* at 1548–49.

[9] *See In re Zappos.com, Inc.*, --- F.3d ----, 2018 WL 1189643 (9th Cir. Mar. 8, 2018); *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. Aug. 1, 2017) *cert. denied*, No. 17-641, 2018 WL 942459 (U.S. Feb. 20, 2018); *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. Appx. 384 (6th Cir. 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015). The Eleventh Circuit also followed a similar approach in *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012), but it is unclear if the Eleventh Circuit would continue to embrace that approach following the U.S. Supreme Court's later decisions in *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013) and *Spokeo, Inc. v. Robins*, 578 U.S. ---, 136 S. Ct. 1540 (2016), which clarified the standards for standing. The Third Circuit has held that statutory standing for a violation of the Fair Credit Reporting Act (FCRA) stemming from a data breach can be sufficient to support standing "[e]ven without evidence that the Plaintiffs' information was in fact used improperly," but the Third Circuit has not addressed whether an increased risk of future injury from a data breach can alone support standing in a data breach case. *See In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 629, 640 (3d Cir. 2017).

[10] --- F.3d ----, 2018 WL 1189643 (9th Cir. Mar. 8, 2018).

[11] *Id.* at *6.

[12] *Id.* at *1, 5. The hacked data did not include social security numbers. The Ninth Circuit noted that the allegations of a separate class of plaintiffs—who had specifically alleged that they *already* suffered identity theft or fraud as a result of the data breach but were not at issue in the appeal—had asserted actual harm by way of identity theft, which "undermines [defendant]'s assertion that the data stolen in the breach cannot be used for fraud or identity theft." *Id.* at *5.

[13] *Id.* at *5 (quoting *Mollan v. Torrance*, 22 U.S. 9 Wheat. 537, 539 (1824)).

[14] 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, No. 17-641, 2018 WL 942459 (U.S. Feb. 20, 2018).

[15] *Id.* at *6.

[16] *Id.* at *6–7. For more information on the *Attias* decision, see our article at: https://www.consumerfinancialserviceswatch.com/2017/08/into-the-breach-d-c-circuit-weighs-in-on-circuit-split-regarding-standing-in-data-breach-class-actions/.

[17] 663 Fed. Appx. 384 (6th Cir. 2016).

[18] *Id.* at 386, 391.

[19] *Id.* at 388.

[20] *Id.* The Sixth Circuit also noted—when assessing the plaintiffs' assertion of standing based upon the prophylactic expenses they incurred to protect their identity after the breach—that the taking of those steps were

reasonable "particularly when [defendant] recommended taking these steps" in its press release regarding the data breach. *Id.* at 388-89.

[21] *See In re SuperValu, Inc.*, 870 F.3d 763, 769–71 (8th Cir. Aug. 30, 2017); *Whalen v. Michaels Stores, Inc.*, 689 Fed. Appx. 89, 2017 WL 1556116 (2d Cir. May 2, 2017) (unpublished); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), *cert. denied*, No. 16-1328, 2017 WL 1740442 (U.S. June 26, 2017). In a pre-*Clapper* and pre-*Spokeo* decision, the First Circuit also appeared to follow this approach when it indicated that mere exposure of the plaintiff's PII could not establish standing, because her allegations do "not identify any incident in which her data has ever been accessed by an unauthorized person." *Katz v. Pershing*, LLC, 672 F.3d 64, 79–80 (1st Cir. 2012) (further noting that plaintiff's standing theory "rests entirely on the hypothesis that at some point an unauthorized, as-yet unidentified, third party might access her data and then attempt to purloin her identity").

[22] 870 F.3d 763 (8th Cir. Aug. 30, 2017).

[23] *Id.* at 766, 769–71.

[24] *Id.* at 770–71 (quoting U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (2007) ("GAO Report")).

[25] *Id.* at 771 (quoting GAO Report at 21).

[26] *Id.* at 769–70 (quoting *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc.*, 528 U.S. 167, 181 (2000)).

[27] *Id.* For more information on the *SuperValu* decision, see our article at: http://www.klgates.com/data-breach-doubleheader-the-eighth-circuit-issues-two-decisions-addressing-boundaries-of-standing-in-data-breach-class-actions-10-09-2017/.

[28] 689 F. App'x 89 (May 2, 2017).

[29] *Id.* at 90.

[30] *Id.* at 90–91.

[31] 848 F.3d 262 (4th Cir. 2017).

[32] *Id.* at 267, 268.

[33] *Id.* at 274.

[34] *Id.* at 275 (quoting *Chambliss v. Carefirst, Inc.*, 189 F.Supp.3d 564, 570 (D. Md. 2016)).

[35] *Id.* at 276.

[36] *See CareFirst, Inc. v. Attias*, No. 17-641, Petition for Writ of Certiorari (U.S. Oct. 30, 2017), https://static.reuters.com/resources/media/editorial/20171031/carefirstdatabreach--certpetition.pdf.

[37] *See* https://www.supremecourt.gov/search.aspx?filename=/docket/DocketFiles/html/Public/17-641.html.

KEY CONTACTS

ANDREW C. GLASS
PARTNER

BOSTON
+1.617.261.3107
ANDREW.GLASS@KLGATES.COM

