DATA BREACH DOUBLEHEADER: THE EIGHTH CIRCUIT ISSUES TWO DECISIONS ADDRESSING BOUNDARIES OF STANDING IN DATA BREACH CLASS ACTIONS

Date: 9 October 2017

U.S. Financial Services/Litigation Alert

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

In two recent decisions, the Eighth Circuit addressed the hotly-litigated issue of when consumer plaintiffs have standing to pursue claims arising out of a data breach. The decisions stake out the Eighth Circuit's positions on a current circuit split and also address the viability of certain types of injuries often alleged in data breach class actions. Notably, the Eighth Circuit revealed its skepticism that an increased risk of future injury alone can support Article III standing in a data breach class action.

In *Kuhns v. Scottrade, Inc.*, [1] the Eighth Circuit expressed approval of a fairly recent and unique standing argument. In *Kuhns*, the plaintiff alleged that hackers stole his personal identifying information ("PII") from the defendant's securities-brokerage system. [2] In assessing plaintiff's standing, the Eighth Circuit focused on his allegation that "a portion of the fees paid in connection with his … account were used to meet [the defendant]'s contractual obligations to provided data management and security to protect his PII." [3] *Kuhns* found this allegation was sufficient to create standing because the plaintiff had alleged that he had "bargained for and expected protection of his PII, that [the defendant] breached the contract when it failed to provide promised reasonable safeguards, and that [the plaintiff] suffered actual injury, the diminished value of his bargain." [4] The court's conclusion that the plaintiffs' benefit-of-the-bargain theory was sufficient to establish standing is contrary to decisions by other courts. [5] The Eighth Circuit reasoned that the standing inquiry is distinct from the inquiry into the viability of a plaintiff's claims, such that "a party to a breached contract has a judicially cognizable interest for standing purposes, regardless of the merits of the breach alleged." [6]

At the same time, the Eighth Circuit roundly *rejected* the same allegation as sufficient to state a breach of contract claim under Rule 12(b)(6). [7] First, the relevant provisions in the defendant's privacy statement were not binding promises but rather "in the nature of contract recitals," which are insufficient to support a breach of contract claim. [8] Second, the language in the privacy statement said that the defendant would "use security measures that comply with federal law," but the plaintiff had not pleaded any federal authority breached by the defendant. [9] Third, the plaintiff had failed to allege any actual damage flowing from the purported breach because he had not claimed that he (or anyone else) had "suffered fraud or identity theft that resulted in financial loss." [10]

Two weeks later, in *In re SuperValu, Inc.*, [11] the Eighth Circuit stepped into the waters on an issue currently dividing the federal circuit courts of appeals—namely whether pleading an increased risk of future injury is sufficient to establish Article III standing in a data breach suit. [12] In *SuperValu*, the plaintiffs alleged that hackers

had stolen their credit and debit card information from the defendant's systems. [13] The vast majority of the plaintiffs alleged only future injury, in the form of an increased risk of identity theft. [14]

The Eighth Circuit did not attempt to reconcile the conflicting circuit court decisions on data breach standing "because the cases ultimately turned on the substance of the allegations before each court." [15] Rather, although recognizing that a "substantial risk of identify theft" may give rise to standing, the court held that the plaintiffs' allegations were insufficient to plead such a risk. [16] First, the *SuperValu* Court rejected as insufficient plaintiffs' allegation that their data was being sold on "illicit websites," because that did not plead any actual harm "to the plaintiffs." [17] Second, the court noted that the information allegedly stolen—credit and debit card information—generally could not 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.'" [18] Third, the plaintiffs had relied upon a report from the U.S. Government Accountability Office ("GAO"), [19] but the court held the report did not support plaintiffs' allegations of future injury as it concluded that "most [data] breaches have not resulted in detected incidents of identity theft." [20] Accordingly, the *SuperValu* Court affirmed dismissal of all of the named plaintiffs who had pleaded only an increased risk of future injury. [21]

The *Kuhns* and *SuperValu* decisions further advance the landscape of authority regarding standing in data breach class actions but also increase the growing divergence between circuits. We will continue to monitor and report on developments in data breach standing law as they occur.

---

[1] 868 F.3d 711 (8th Cir. 2017).

[2] *Id.* at 714-15.

[3] *Id.* at 716.

[4] *Id.*

[5] *See Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016) (finding no standing where plaintiffs "offer no factual allegations indicating that the prices they paid for health insurance included a sum to be used for data security"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014); *Lewert v. P.F. Chang's China Bistro, Inc.*, 2014 WL 7005097, at *2 (N.D. Ill. Dec. 10, 2014) (dismissing action for lack of standing where plaintiffs merely argued "the cost of the food they purchased implicitly contained the cost of sufficient protection of PII"), *rev'd on other grounds*, 2016 WL 1459226 (7th Cir. Apr. 14, 2016). For more on the "benefit of the bargain" theory of standing in data breach cases, 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/.

[6] *Kuhns*, 868 F.3d at 716 (quoting *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 909 (8th Cir. 2016)).

[7] *Id.* at 717-19 (holding that "the allegation that the failure of [defendant's] security measures was a breach of contract that diminished the benefit of [plaintiff's] bargain is not plausible").

[8] *Id.* at 717.

[9] *Id.*

[10] *Id.* at 718.

[11] 870 F.3d 763 (8th Cir. Aug. 30, 2017).

[12] Some circuit courts agree with the Eighth Circuit that data breach plaintiffs lack standing where they plead nothing more than an increased risk of future injury. *See 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). Other circuit courts, however, have approved of standing based solely on an increased risk of future injury stemming from a data breach. *See Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. Aug. 1, 2017); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012); *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); and *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015)

[13] *In re SuperValu, Inc.*, 870 F.3d at 766-67.

[14] *Id.* at 767.

[15] *Id.* at 769. The heavily fact-specific nature of whether standing has been adequately pleaded in data breach class actions is borne out by two recent decisions in the D.C. Circuit. In August 2017, the D.C. Circuit held that plaintiffs had adequately alleged substantial risk of future injury where a data breach had exposed their information, and it was plausible that the unauthorized party had "the intent and the ability to use [the] data for ill." *See Attias v. Carefirst, Inc.*, 865 F.3d 620, 622, 628-29 (D.C. Cir. 2017); *see also* www.consumerfinancialserviceswatch.com/2017/08/into-the-breach-d-c-circuit-weighs-in-on-circuit-split-regarding-standing-in-data-breach-class-actions/. Just over a month later, the D.C. District Court found standing lacking, because "plaintiffs cannot predicate standing on the basis of the breach alone," and the plaintiffs had not adequately alleged that they suffered actual injury or faced a substantial risk of future injury from the breach. *See In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, No. MC 15-1394, 2017 WL 4129193, at *11-24 (D.D.C. Sept. 19, 2017).

[16] *In re SuperValu, Inc.*, 870 F.3d at 769-71.

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

[18] *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")).

[19] *See* GAO Report.

[20] *In re SuperValu, Inc.*, 2017 WL 3722455 at 771 (quoting GAO Report at 21).

[21] *Id.* at 774. The Eighth Circuit reversed the dismissal as to one named plaintiff, who had pleaded that a fraudulent charge had been made to his credit card.

KEY CONTACTS

ANDREW C. GLASS
PARTNER
BOSTON
+1.617.261.3107
ANDREW.GLASS@KLGATES.COM

