

870 F.3d 763
United States Court of Appeals,
Eighth Circuit.

IN RE: SUPERVALU, INC., Customer
Data Security Breach Litigation
Melissa Alleruzzo; Heidi Bell; Rifet Bosnjak;
John Gross; Kenneth Hanff; David Holmes;
Steve McPeak; Gary Mertz; Katherin Murray;
Christopher Nelson; Carol Puckett; Alyssa
Rocke; Timothy Roldan; Ivanka Soldan; Melissa
Thompkins; Darla Young, Plaintiffs-Appellants,
v.

SuperValu, Inc.; AB Acquisition, LLC; New
Albertsons, Inc., Defendants-Appellees.
Electronic Privacy Information Center
Amicus on Behalf of Appellant(s)
In re: SuperValu, Inc., Customer
Data Security Breach Litigation
Melissa Alleruzzo; Heidi Bell; Rifet Bosnjak;
John Gross; Kenneth Hanff; David Holmes;
Steve McPeak; Gary Mertz; Katherin Murray;
Christopher Nelson; Carol Puckett; Alyssa
Rocke; Timothy Roldan; Ivanka Soldan; Melissa
Thompkins; Darla Young, Plaintiffs-Appellees,
v.

SuperValu, Inc.; AB Acquisition, LLC; New
Albertsons, Inc., Defendants-Appellants.

No. 16-2378, No. 16-2528

|
Submitted: May 10, 2017

|
Filed: August 30, 2017

Synopsis

Background: Customers, whose financial information was allegedly accessed and stolen in data breach, brought putative class actions against owners and operators of grocery stores, alleging violations of state consumer protection statutes, violations of state data breach notification statutes, negligence, breach of implied contract, negligence per se, and unjust enrichment. The United States District Court for the District of Minnesota, *Ann D. Montgomery, J., 2016 WL 81792*, dismissed. Customers appealed.

Holdings: The Court of Appeals, Kelly, Circuit Judge, held that:

[1] complaint failed to allege substantial risk of identity theft, but

[2] customer had standing.

Affirmed in part, reversed in part, and remanded.

West Headnotes (12)

[1] Federal Courts

🔑 Case or Controversy Requirement

Article III of the Constitution limits the jurisdiction of the federal courts to cases or controversies. *U.S. Const. art. 3, § 2, cl. 1.*

[Cases that cite this headnote](#)

[2] Federal Civil Procedure

🔑 In general;injury or interest

Federal Civil Procedure

🔑 Causation;redressability

A plaintiff invoking the jurisdiction of the court must demonstrate standing to sue by showing that she has suffered an injury in fact that is fairly traceable to the defendant's conduct and that is likely to be redressed by the relief she seeks.

[Cases that cite this headnote](#)

[3] Federal Civil Procedure

🔑 In general;injury or interest

To establish an injury in fact, as required for standing, a plaintiff must show that her injury is concrete and particularized and actual or imminent, not conjectural or hypothetical.

[Cases that cite this headnote](#)

[4] Federal Civil Procedure

🔑 [Causation;redressability](#)

An injury is fairly traceable, as required for standing, if the plaintiff shows a causal connection between the injury and the conduct complained of that is not the result of the independent action of some third party not before the court.

[Cases that cite this headnote](#)

[5] **Federal Courts**

🔑 [Standing](#)

Federal Courts

🔑 [Pleadings;Dismissal](#)

Where defendants facially attacked plaintiffs' standing, appellate court reviews the district court's dismissal for lack of standing de novo, accepting the material allegations in the complaint as true and drawing all inferences in plaintiffs' favor.

[Cases that cite this headnote](#)

[6] **Federal Civil Procedure**

🔑 [Representation of class;typicality; standing in general](#)

The requirements for standing do not change in the class action context.

[Cases that cite this headnote](#)

[7] **Federal Civil Procedure**

🔑 [Representation of class;typicality; standing in general](#)

A putative class action can proceed as long as one named plaintiff has standing.

[Cases that cite this headnote](#)

[8] **Antitrust and Trade Regulation**

🔑 [Private entities or individuals](#)

Consumer Credit

🔑 [Actions;injunction](#)

Federal Civil Procedure

🔑 [Consumers, purchasers, borrowers, and debtors](#)

Complaint failed to adequately allege injury in fact, that customers faced substantial risk of identity theft as a result of data breaches purportedly caused by deficient security practices of owners and operators of grocery stores, and thus customers did not have standing to bring putative class action for, inter alia, violations of state consumer protection statutes, violations of state data breach notification statutes, negligence, and breach of implied contract; allegedly stolen credit and debit card information did not include any personally identifying information, such as social security numbers, birth dates, or driver's license numbers, there was little to no risk that anyone would use stolen card information to open unauthorized accounts in customers' names, and report of United States Government Accountability Office (GAO) found that data breaches were unlikely to result in identity theft.

[Cases that cite this headnote](#)

[9] **Federal Civil Procedure**

🔑 [In general;injury or interest](#)

In future injury cases, a plaintiff must demonstrate that the threatened injury is certainly impending, or there is a substantial risk that the harm will occur, in order to have standing.

[Cases that cite this headnote](#)

[10] **Antitrust and Trade Regulation**

🔑 [Private entities or individuals](#)

Consumer Credit

🔑 [Actions;injunction](#)

Federal Civil Procedure

🔑 [Consumers, purchasers, borrowers, and debtors](#)

Customer, whose financial information was allegedly accessed and stolen in data breach, had standing to bring putative class action against owners and operators of grocery stores for, inter alia, violations of state consumer protection statutes, violations of state data breach notification statutes,

negligence, and breach of implied contract; customer alleged that he suffered fraudulent charge on credit card he previously used to make purchase at grocery store affected by data breach, misuse of card information was credit card fraud and form of identity theft, customer alleged fraudulent charge was fairly traceable to breaches, and to the extent customer could show that fraudulent charge was unreimbursed, such financial harm would be compensable in action.

[Cases that cite this headnote](#)

[11] Federal Civil Procedure

🔑 [Theory of claim](#)

It is unnecessary to set out a legal theory for the plaintiff's claim for relief in a pleading.

[Cases that cite this headnote](#)

[12] Federal Civil Procedure

🔑 [In general;injury or interest](#)

Each plaintiff's standing must be assessed individually.

[Cases that cite this headnote](#)

***765** Appeals from United States District Court for the District of Minnesota—Minneapolis

Attorneys and Law Firms

[Ben Barnow](#), Barnow & Associates, [Aron Robinson](#), Law Offices of Aron D. Robinson, Chicago, IL, [Richard L. Coffman](#), Coffman Law Firm, Beaumont, TX, [John J. Driscoll](#), [Christopher Joseph Quinn](#), The Driscoll Firm, [John S. Steward](#), Steward Law Firm, Saint Louis, MO, [Edwin J. Kilpela, Jr.](#), Carlson & Lynch, Pittsburgh, PA, [David Langevin](#), Mcsweeney & Fay, [Karen Riebel](#), Lockridge & Grindal, Minneapolis, MN for Plaintiffs-Appellees.

[Katherine Susan Barrett Wiik](#), [Stephen Paul Safranski](#), ROBINS & KAPLAN, Minneapolis, MN, [David Thomas Cohen](#), Ropes & Gray, New York, NY, [Kathryn](#)

[Elizabeth Wilhelm](#), [Harvey J. Wolkoff](#), Ropes & Gray, Boston, MA for Defendant-Appellant SuperValu, Inc.

[Marc Andre Al](#), Stoel & Rives, Minneapolis, MN, [Christopher L. Ingram](#), [John L. Landolfi](#), Vorys & Sater, Columbus, OH for Defendants-Appellants AB Acquisition, LLC, New Albertsons, Inc.

Alan Jay Butler, Senior Counsel, [Marc Rotenberg](#), Aimee Thomson, Electronic Privacy Information Center, Washington, DC for Amicus on Behalf of Appellant(s).

Before [SMITH](#), Chief Judge, [COLLTON](#) and [KELLY](#), Circuit Judges.

Opinion

[KELLY](#), Circuit Judge.

In 2014, retail grocery stores owned and operated by defendants SuperValu, Inc., AB Acquisition, LLC, and New Albertsons, Inc. suffered two cyber attacks in which their customers' financial information was allegedly accessed and stolen. Following the data breaches, customers who shopped at the affected stores brought several putative class actions, which were subsequently centralized in the United States District Court for the District of Minnesota by the Judicial Panel on Multidistrict Litigation. The district court dismissed the plaintiffs' consolidated complaint under [Federal Rule of Civil Procedure 12\(b\)\(1\)](#), concluding that plaintiffs failed to allege facts establishing Article III standing. Plaintiffs appealed, and we affirm in part, reverse in part, and remand for further proceedings.

***766 I. Background**

The following facts, which we accept as true, are drawn from the consolidated amended complaint and the appended exhibits. See [Carlsen v. GameStop, Inc.](#), 833 F.3d 903, 908 (8th Cir. 2016). Plaintiffs are sixteen customers who purchased goods from defendants' grocery stores in Missouri, Illinois, Maryland, Pennsylvania, Delaware, Idaho, and New Jersey using credit or debit cards during the period between June and September 2014. From June 22, 2014, to July 17, 2014, cyber criminals accessed the computer network that processes payment card transactions for 1,045 of defendants' stores. The hackers installed malicious software on defendants' network that allowed them to gain access to the payment

card information of defendants' customers (hereinafter, Card Information), including their names, credit or debit card account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs). By harvesting the data on the network, the hackers stole customers' Card Information.

On August 14, 2014, defendants issued a press release notifying customers of the computer intrusion at their stores. The press release acknowledged that the attack "may have resulted in the theft" of Card Information, but it had not yet been determined that "any such cardholder data was in fact stolen," and, at that point, there was "no evidence of any misuse of any such data." Defendants also announced that they were conducting an on-going investigation into the incident, which might uncover additional "time frames, locations and/or at-risk data" exposed in the intrusion.

On September 29, 2014, defendants announced a second data breach that took place in late August or early September 2014. The press release stated that an intruder installed different malicious software onto the same network. Defendants acknowledged that the software may have captured Card Information from debit and credit cards used to purchase goods at their stores but, at the time of the press release, there had been no determination that such information "was in fact stolen." Once again, defendants affirmed that their investigation was ongoing, and that further information on the scope of the intrusion could be identified in the future. Although defendants' release states that the second intrusion was separate from the one announced on August 14, 2014, plaintiffs dispute this contention in their complaint, alleging that the two breaches were related and stemmed from the same security failures.

According to the complaint, hackers gained access to defendants' network because defendants failed to take adequate measures to protect customers' Card Information. Defendants used default or easily guessed passwords, failed to lock out users after several failed login attempts, and did not segregate access to different parts of the network or use firewalls to protect Card Information. By not implementing these measures, defendants ran afoul of best practices and industry standards for merchants who accept customer payments via credit or debit card. Moreover, defendants were on notice of the risk of consumer data theft because similar security flaws had

been exploited in recent data breaches targeting other national retailers.

As a result of the breaches, plaintiffs' Card Information was allegedly stolen, subjecting plaintiffs "to an imminent and real possibility of identity theft." Specifically, plaintiffs contend that the hackers can use their Card Information to siphon money from their current accounts, make unauthorized credit or debit card charges, *767 open new accounts, or sell the information to others who intend to commit fraud. Identity thieves can use the stolen Card Information to commit fraud for an "extended period of time after" the breach, and the information is often traded on the cyber black market "for a number of years after the initial theft." In support of these allegations, plaintiffs cite a June 2007 United States Government Accountability Office (GAO) report on data breaches. See 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), <http://www.gao.gov/assets/270/262899.pdf>.

Customers allegedly affected by the breaches filed putative class actions in several district courts. The Judicial Panel on Multidistrict Litigation transferred the related actions to the United States District Court for the District of Minnesota for coordinated or consolidated pretrial proceedings. Pursuant to the district court's order, plaintiffs filed a consolidated amended complaint on June 26, 2015, with sixteen named plaintiffs bringing claims on behalf of a putative class of persons affected by defendants' data breaches.

Each of the sixteen plaintiffs shopped at defendants' affected stores using a credit or debit card, and their Card Information was allegedly compromised in the data breaches. After the data breaches were announced, each plaintiff "spent time determining if [his or her] card was compromised" by reviewing information released about the breaches and the impacted locations and monitoring account information to guard against potential fraud. Crucial to the outcome in this appeal, one plaintiff, David Holmes, used his credit card at a store in Belleville, Illinois¹ that was affected by the data breaches, and alleges his Card Information was compromised as a result of defendants' security failures. Shortly after the data breach was announced, "Holmes noticed a fraudulent charge on his credit card statement and immediately

cancelled his credit card, which took two weeks to replace.”

The complaint states six claims for relief for: (1) violations of state consumer protection statutes, (2) violations of state data breach notification statutes, (3) negligence, (4) breach of implied contract, (5) negligence per se, and (6) unjust enrichment. Defendants moved to dismiss the complaint under [Federal Rules of Civil Procedure 12\(b\)\(1\) and 12\(b\)\(6\)](#). The district court granted the [Rule 12\(b\)\(1\)](#) motion and dismissed the complaint without prejudice, finding that none of the plaintiffs had alleged an injury-in-fact and thus they did not have standing. The court did not address defendants' arguments for dismissal under [Rule 12\(b\)\(6\)](#).² Plaintiffs appeal the district court's dismissal, and defendants cross-appeal, arguing that the complaint was alternatively subject to dismissal with prejudice under [Rule 12\(b\)\(6\)](#).

II. Discussion

[1] [2] [3] [4] Article III of the Constitution limits the jurisdiction of the federal courts to cases or controversies. *768 [Spokeo, Inc. v. Robins](#), — U.S. —, 136 S.Ct. 1540, 1547, 194 L.Ed.2d 635 (2016). A plaintiff invoking the jurisdiction of the court must demonstrate standing to sue by showing that she has suffered an injury in fact that is fairly traceable to the defendant's conduct and that is likely to be redressed by the relief she seeks. [Id.](#) This case primarily concerns the injury in fact and fairly traceable elements. To establish an injury in fact, a plaintiff must show that her injury is “‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” [Id.](#) at 1548 (quoting [Lujan v. Defs. of Wildlife](#), 504 U.S. 555, 560, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992)). An injury is fairly traceable if the plaintiff shows “a causal connection between the injury and the conduct complained of” that is “not ... th[e] result [of] the independent action of some third party not before the court.” [Lujan](#), 504 U.S. at 560, 112 S.Ct. 2130 (alterations in original) (internal quotation omitted).

[5] Because this case is at the pleading stage, plaintiffs “must ‘clearly allege facts’ demonstrating” the elements of standing. [Spokeo](#), 136 S.Ct. at 1547 (alteration omitted) (quoting [Warth v. Seldin](#), 422 U.S. 490, 518, 95 S.Ct. 2197, 45 L.Ed.2d 343 (1975)). Where, as here, defendants facially attacked plaintiffs' standing, we review the district

court's dismissal for lack of standing de novo, accepting the material allegations in the complaint as true and drawing all inferences in plaintiffs' favor. [See Carlsen](#), 833 F.3d at 908.

[6] [7] The requirements for standing do not change in the class action context. [See Spokeo](#), 136 S.Ct. at 1547 n.6. A putative class action can proceed as long as one named plaintiff has standing. [See Horne v. Flores](#), 557 U.S. 433, 446, 129 S.Ct. 2579, 174 L.Ed.2d 406 (2009); [Arlington Heights v. Metro. Hous. Dev. Corp.](#), 429 U.S. 252, 264 & n.9, 97 S.Ct. 555, 50 L.Ed.2d 450 (1977). “Accordingly, at least one of the [sixteen] named Plaintiffs must have Article III standing in order to maintain this class action.” [In re Horizon Healthcare Servs. Inc. Data Breach Litig.](#), 846 F.3d 625, 634 (3d Cir. 2017); [see O'Shea v. Littleton](#), 414 U.S. 488, 494, 94 S.Ct. 669, 38 L.Ed.2d 674 (1974) (“[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class.”).

The district court evaluated the standing of all the named plaintiffs collectively. As relevant here, the court concluded that because the complaint alleged only an “isolated single instance of an unauthorized charge” suffered by plaintiff Holmes, there was insufficient evidence of misuse of plaintiffs' Card Information connected to defendants' data breaches to “plausibly suggest [] that the hackers had succeeded in stealing the data and were willing and able to use it for future theft or fraud.” On appeal, plaintiffs argue that they have sufficiently alleged an injury in fact because the theft of their Card Information in the data breaches at defendants' stores created a substantial risk that they will suffer identity theft in the future. In addition, plaintiff Holmes specifically argues that his allegations of actual misuse of his Card Information are sufficient to allege a present injury in fact causally connected to defendants' careless security practices. Although we conclude that the complaint does not sufficiently allege a substantial risk of future identity theft, we nonetheless find that the court has subject matter jurisdiction over this action because plaintiff Holmes has alleged facts giving rise to standing.

A. Future Injury

[8] [9] Plaintiffs argue that they have sufficiently alleged an injury in fact because *769 the theft of their Card Information due to the data breaches at defendants' stores

creates the risk that they will suffer identity theft in the future. The Supreme Court has recognized that future injury can be sufficient to establish Article III standing. See [Clapper v. Amnesty Int'l USA](#), 568 U.S. 398, 409, 133 S.Ct. 1138, 185 L.Ed.2d 264 (2013). In future injury cases, the plaintiff must demonstrate that “the threatened injury is ‘certainly impending,’ or there is a ‘substantial risk’ that the harm will occur.” [Susan B. Anthony List v. Driehaus](#), — U.S. —, 134 S.Ct. 2334, 2341, 189 L.Ed.2d 246 (2014) (quoting [Clapper](#), 568 U.S. at 409, 414 n.5, 133 S.Ct. 1138).³ The question here is whether the complaint adequately alleges that plaintiffs face a “certainly impending” or “substantial risk” of identity theft as a result of the data breaches purportedly caused by defendants' deficient security practices.

Although we have not had occasion to address this question, several circuits have applied [Clapper](#) to determine whether an increased risk of future identity theft constitutes an injury in fact. See [Attias](#), 865 F.3d at 625-29, 2017 WL 3254941, at *3-7; [Whalen v. Michaels Stores, Inc.](#), No. 16-260 (L), 689 Fed.Appx. 89, 89-91, 2017 WL 1556116, at *1-2 (2d Cir. May 2, 2017) (Summ. Order); [Beck](#), 848 F.3d at 273-76; [Galaria v. Nationwide Mut. Ins.](#), 663 Fed.Appx. 384, 387-90 (6th Cir. 2016); [Lewert v. P.F. Chang's China Bistro, Inc.](#), 819 F.3d 963, 966-69 (7th Cir. 2016); [Remijas v. Neiman Marcus Grp., LLC](#), 794 F.3d 688, 692-93 (7th Cir. 2015). These cases came to differing conclusions on the question of standing. We need not reconcile this out-of-circuit precedent because the cases ultimately turned on the substance of the allegations before each court. Thus, we begin with the facts pleaded by plaintiffs here.

Defendants argue that plaintiffs have at most alleged only that the intruders accessed the card data, not that they stole it. We disagree. At several points, the complaint alleges that the malware the hackers installed on defendants' network allowed them to “harvest” plaintiffs' Card Information, that defendants' security practices “allow[ed] and ma[de] possible the theft” of plaintiffs' Card Information, and that plaintiffs have actually “suffered theft” of their Card Information. Moreover, defendants' own press releases, which are appended to the complaint, acknowledge that the data breaches “may have resulted in the theft of” Card Information. Defendants argue that the allegations are conclusory, but “on a motion to dismiss we presum[e] that general allegations embrace those specific facts that are

necessary to support the claim.” [Lujan](#), 504 U.S. at 561, 112 S.Ct. 2130 (alteration in original) (internal quotation omitted). Drawing all inferences in the plaintiffs' favor, we are satisfied that the complaint sufficiently alleges that the hackers stole plaintiffs' Card Information.

Plaintiffs, however, ask us to go further and conclude that the complaint has adequately alleged that their Card Information has been misused. With the exception of plaintiff Holmes, discussed further below, the named plaintiffs have not alleged that they have suffered fraudulent charges on their credit or debit cards or that fraudulent accounts have been opened in their *770 names. Plaintiffs point to the allegations that, on information and belief, illicit websites are selling their Card Information to counterfeiters and fraudsters, and that plaintiffs' financial institutions are attempting to mitigate their risk. Not only are these allegations speculative, they also fail to allege any injury “to the plaintiff[s].” [Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. \(TOC\), Inc.](#), 528 U.S. 167, 181, 120 S.Ct. 693, 145 L.Ed.2d 610 (2000); see [Spokeo](#), 136 S.Ct. at 1548 (injury “must affect the plaintiff in a personal and individual way” (quoting [Lujan](#), 504 U.S. at 560 n.1, 112 S.Ct. 2130)). Therefore, setting aside Holmes, plaintiffs sufficiently allege that their Card Information was stolen by hackers as a result of defendants' security practices, but not that it was misused.

Plaintiffs argue that the theft of their Card Information creates a substantial risk that they will suffer identity theft. According to the GAO report cited in the complaint, “identity theft” “encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name.” U.S. Gov't Accountability Off., [supra](#), at 2. Defendants appear to concede that identity theft constitutes an actual, concrete, and particularized injury. See [Attias](#), 865 F.3d at 627, 2017 WL 3254941, at *5 (“Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury.”). Our task is to determine whether plaintiffs' allegations plausibly demonstrate that the risk that plaintiffs will suffer future identity theft is substantial.

Although others have ruled that a complaint could plausibly plead that the theft of a plaintiff's personal

or financial information creates a substantial risk that they will suffer identity theft sufficient to constitute a threatened injury in fact, *see, e.g., Remijas*, 794 F.3d at 692–93, we conclude that plaintiffs have not done so here. As factual support for the otherwise bare assertion that “[d]ata breaches facilitate identity theft,” the complaint relies solely on the 2007 GAO report.⁴ *See generally* U.S. Gov’t Accountability Off., *supra*. This report fails to support plaintiffs’ contention.

Initially, we note that the allegedly stolen Card Information does not include any personally identifying information, such as social security numbers, birth dates, or driver’s license numbers. As the GAO report points out, compromised credit or debit card information, like the Card Information here, “generally cannot be used alone to open unauthorized new accounts.” *Id.* at 30 (“The type of data compromised in a breach can effectively determine the potential harm that can result.”). As such, pursuant to the factual evidence relied on in the complaint, there is little to no risk that anyone will use the Card Information stolen in these data breaches 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.” *Id.* We are left with the risk that plaintiffs’ Card Information could be used to commit credit or debit card fraud, in which criminals *771 make unauthorized charges to or siphon money from those existing accounts.

Ultimately, the findings of the GAO report do not plausibly support the contention that consumers affected by a data breach face a substantial risk of credit or debit card fraud. Although the report acknowledges that there are some cases in which a data breach appears to have resulted in identity theft, it concludes based on the “available data and information” that “most breaches have not resulted in detected incidents of identity theft.” *Id.* at 21. Among other evidence, the report reviews the 24 largest data breaches reported between January 2000 and June 2005, and finds only four were known to have resulted in some form of identity theft, and only three of those were believed to be incidents of account fraud. *Id.* at 24–25. Because the report finds that data breaches are unlikely to result in account fraud, it does not support the allegation that defendants’ data breaches create a substantial risk that plaintiffs will suffer credit or debit card fraud. *See Beck*, 848 F.3d at 276.

The 2007 report found that “[c]omprehensive information on the outcomes of data breaches is not available,” U.S. Gov’t Accountability Off., *supra* at 21, and the “extent to which data breaches result in identity theft is not well known,” *id.* at 5. It is possible that some years later there may be more detailed factual support for plaintiffs’ allegations of future injury. But such support is absent from the complaint here, and a mere possibility is not enough for standing.⁵ *See Clapper*, 568 U.S. at 409, 133 S.Ct. 1138 (“[A]llegations of possible future injury’ are not sufficient.” (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158, 110 S.Ct. 1717, 109 L.Ed.2d 135 (1990))); *Braitberg v. Charter Commc’ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) (“[A] speculative or hypothetical risk is insufficient.”).

Plaintiffs also argue that the costs they incurred to mitigate their risk of identity theft, including time they spent reviewing information about the breach and monitoring their account information, constitute an injury in fact for purposes of standing. Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury. *See Clapper*, 133 S.Ct. at 1151 (plaintiffs “cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending”); *Beck*, 848 F.3d at 276–77 (“[S]elf-imposed harms cannot confer standing.”).⁶

Accordingly, we conclude that the complaint has not sufficiently alleged a *772 substantial risk of identity theft, and plaintiffs’ allegations of future injury do not support standing in this case.

B. Present Injury

[10] Although the complaint’s allegations of future injury are insufficient, plaintiff Holmes alleges a present injury in fact to support his standing. He alleges that he suffered a fraudulent charge on the credit card he previously used to make a purchase at one of defendants’ stores affected by the data breaches. This misuse of Holmes’ Card Information is credit card fraud and thus a form of identity theft. As previously noted, defendants do not contest that identity theft constitutes an actual, concrete, and particularized injury. *See Attias*, 865 F.3d at 626–28, 2017 WL 3254941, at *5. Instead of attacking the nature

of Holmes' injury, defendants challenge the sufficiency of his allegations.

[11] First, defendants argue that Holmes' theory of actual injury “is not properly before the Court because it is not alleged in the Complaint.” Contrary to defendants' contention, “it is unnecessary to set out a legal theory for the plaintiff's claim for relief” in a pleading. [Johnson v. City of Shelby](#), —U.S. —, 135 S.Ct. 346, 347, 190 L.Ed.2d 309 (2014) (internal quotation omitted). So long as the facts alleged in the complaint demonstrate Holmes' actual injury, plaintiffs have met their burden at the pleading stage. Cf. [Topchian v. JPMorgan Chase Bank, N.A.](#), 760 F.3d 843, 849 (8th Cir. 2014) (“[I]t is the facts alleged in a complaint, and not the legal theories, that state a claim.”).

Second, defendants argue that Holmes has not sufficiently alleged that his injury is fairly traceable to defendants' data breaches for essentially two reasons. Initially, defendants contend that Holmes must allege that his particular “fraudulent charge occurred because of” defendants' data breaches. By focusing narrowly on the allegations specific to Holmes, defendants ignore the allegations in the complaint that apply to all plaintiffs. These latter allegations state a “causal connection,” [Bennett v. Spear](#), 520 U.S. 154, 167, 117 S.Ct. 1154, 137 L.Ed.2d 281 (1997), between the deficiencies in defendants' security system and the theft and misuse of customers' Card Information: Defendants failed to secure customer Card Information on their network; their network was subsequently hacked; customer Card Information was stolen by the hackers; and Holmes became the victim of identity theft after the data breaches. At this stage of the litigation, “we presum[e] that [these] general allegations embrace those specific facts that are necessary to support” a link between Holmes' fraudulent charge and the data breaches. *Id.* at 168, 117 S.Ct. 1154 (first alteration in original) (quoting [Lujan](#), 504 U.S. at 561, 112 S.Ct. 2130). We thus find Holmes has met his burden, “which is relatively modest at this stage of the litigation,” of alleging that his fraudulent charge is fairly traceable to the defendants' breaches. *Id.* at 171, 117 S.Ct. 1154; see [Resnick v. AvMed, Inc.](#), 693 F.3d 1317, 1324 (11th Cir. 2012) (concluding that actual identity fraud following the theft of laptops containing plaintiffs' personal information was fairly traceable to defendant's failures).

In addition, defendants argue that the fairly traceable element is not satisfied because without evidence of widespread misuse, the complaint does not support the inference that these data breaches caused Holmes' fraudulent charge. Defendants rely on the district court's “common sense” conclusion that due to the frequency of credit card fraud, one would expect that in a group of sixteen named plaintiffs and thousands of potential class members who used a credit or debit card at defendants' *773 affected stores, there would be more than one instance of a fraudulent charge. After finding that evidence of misuse was required to establish standing, the district court concluded that “the single isolated instance of an unauthorized charge [suffered by Holmes] is not indicative of data misuse that is fairly traceable to the Data Breach.”

[12] Even if evidence of misuse following a data breach is necessary for a plaintiff to establish standing—a conclusion we need not definitively reach today—we conclude that the district court erred in holding that Holmes' standing was dependent on the standing of other named plaintiffs and unnamed class members. Each plaintiff's standing must be assessed individually. See [Red River Freethinkers v. City of Fargo](#), 679 F.3d 1015, 1023 (8th Cir. 2012) (standing requires examination of “whether the particular plaintiff is entitled to an adjudication of the particular claims asserted” (quoting [Allen v. Wright](#), 468 U.S. 737, 752, 104 S.Ct. 3315, 82 L.Ed.2d 556 (1984))); [Jones v. Gale](#), 470 F.3d 1261, 1265 (8th Cir. 2006) (“[W]here one plaintiff establishes standing to sue, the standing of other plaintiffs is immaterial to jurisdiction.” (internal quotation omitted)). At a later stage of the litigation, defendants are free to litigate whether the data breach caused Holmes' fraudulent charge, but “this debate has no bearing on standing to sue.” [Remijas](#), 794 F.3d at 696; see [Lexmark Int'l, Inc. v. Static Control Components, Inc.](#), — U.S. —, 134 S.Ct. 1377, 1391 n.6, 188 L.Ed.2d 392 (2014) (“Proximate causation is not a requirement of Article III standing.”).

Holmes' allegations of misuse of his Card Information were sufficient to demonstrate that he had standing; that is all that is required for the court to have subject matter jurisdiction over this action. See 2 [William B. Rubenstein, Newberg on Class Actions](#) § 2:1 (5th ed. 2012) (“Once threshold individual standing by the class representative is met, a proper party to raise a particular issue is before the court; there is no further, separate ‘class action

standing’ requirement.”); cf. [Spokeo](#), 136 S.Ct. at 1547 n.6 (“[N]amed plaintiffs who represent a class must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong.” (internal quotation omitted)).

Finally, defendants point to several purported deficiencies in Holmes' allegations, arguing that he failed to allege the date he shopped at the affected Illinois store, the amount of the charge, or that the charge was unreimbursed. While such omissions could be fatal to the complaint under the “higher hurdles” of [Rules 8\(a\)](#) and [12\(b\)\(6\)](#)—a contention that we do not opine on here—standing under Article III presents only a “threshold inquiry,” [Brown v. Medtronic, Inc.](#), 628 F.3d 451, 459 (8th Cir. 2010), requiring “general allegations” of injury, causation, and redressability, [Lujan](#), 504 U.S. at 561, 112 S.Ct. 2130. We conclude that these attacks on the sufficiency of Holmes' allegations are more properly directed at whether the complaint states a claim, not whether Holmes has alleged standing. See [Miller v. Redwood Toxicology Lab., Inc.](#), 688 F.3d 928, 936 (8th Cir. 2012) (“The issue ... of whether Miller's allegations are sufficient to state a cause of action under [Rule 12\(b\)\(6\)](#) presents a different and distinct matter” from Article III standing).

Although defendants do not challenge the final element of standing, we find that Holmes' injury is “likely to be redressed by a favorable judicial decision.” [Spokeo](#), 136 S.Ct. at 1547. To the extent Holmes can show that the fraudulent charge was unreimbursed, such financial harm

would be compensable in this action. See *774 [Remijas](#), 794 F.3d at 696–97; see also [Warth](#), 422 U.S. at 500, 95 S.Ct. 2197 (“[S]tanding in no way depends on the merits of the plaintiffs’ claim”).

Because the complaint contains sufficient allegations to demonstrate that Holmes suffered an injury in fact, fairly traceable to defendants' security practices, and likely to be redressed by a favorable judgment, Holmes has standing under Article III's case or controversy requirement. See [Lewert](#), 819 F.3d at 967 (named plaintiff who “asserts that he already has experienced fraudulent charges” and “has spent time and effort resolving them” has “alleged sufficient facts to support standing based on [his] present injuries”); [Resnick](#), 693 F.3d at 1323 (“[A] party claiming actual identity theft resulting from a data breach has standing to bring suit.”). Since one named plaintiff has standing to bring suit, the district court erred in dismissing the action for lack of subject matter jurisdiction.⁷

III. Conclusion

For the foregoing reasons, we reverse the district court's dismissal of plaintiff Holmes for lack of Article III standing, affirm the dismissal as to the remaining plaintiffs, and remand for further proceedings consistent with this order.

All Citations

870 F.3d 763

Footnotes

- 1 Although some of the other named plaintiffs allege the specific dates that they shopped, plaintiff Holmes does not include the date, but does identify the store name and location.
- 2 After the entry of judgment, plaintiffs moved to alter or amend pursuant to [Rule 59\(e\)](#), attaching, for the first time, declarations from officers of financial institutions. Because plaintiffs did not appeal the district court's denial of the [Rule 59\(e\)](#) motion, we do not consider the arguments raised in the motion or the exhibits attached thereto. See [Gannon Int'l, Ltd. v. Blocker](#), 684 F.3d 785, 793–94 (8th Cir. 2012).
- 3 Defendants argue that we should apply only the “certainly impending” formulation of the future injury test. The Supreme Court has at least twice indicated that both the “certainly impending” and “substantial risk” standards are applicable in future injury cases, albeit without resolving whether they are distinct, and we are obligated to follow this precedent. See [Driehaus](#), 134 S.Ct. at 2341, 2345–46; [Clapper](#), 568 U.S. at 409, 414 n.5, 133 S.Ct. 1138; see also [Attias v. Carefirst, Inc.](#), 865 F.3d 620, 626–28, 2017 WL 3254941, at *5 (D.C. Cir. 2017); [Beck v. McDonald](#), 848 F.3d 262, 272, 275 (4th Cir. 2017).
- 4 The complaint does cite a booklet prepared by the Federal Trade Commission, but this document only provides steps to take if a person is or suspects she may be a victim of identity theft. See Fed. Trade Comm'n, *Taking Charge: What*

To Do If Your Identity Is Stolen (2013), <https://publications.usa.gov/USAPubs.php?PubID=3326>. This document has no bearing on the risk of identity theft following a data breach.

5 We recognize there may be other means—aside from relying on reports and studies—to allege a substantial risk of future injury, and we do not comment on the sufficiency of such potential methods here. We also do not address any of the independent forms of injury discussed by the district court, including the argument that the invasion of privacy suffered by the plaintiffs constitutes an injury in fact, because the plaintiffs do not press them on appeal.

6 Plaintiffs also cursorily argue that because they have alleged in claim four that defendants breached an implied contract to “take reasonable measures to protect” plaintiffs’ Card Information, the complaint adequately alleges standing. We have held, in the context of an express contract, that “a plaintiff who has produced facts indicating it was a party to a breached contract has a judicially cognizable interest for standing purposes, regardless of the merits of the breach alleged.” [Carlsen](#), 833 F.3d at 909 (internal quotation omitted). Even if such analysis applies to an implied contract—a question we need not decide here—the complaint does not sufficiently allege that plaintiffs were party to such a contract. Therefore, the breach of implied contract claim does not supply plaintiffs with Article III standing.

7 In their cross appeal, Defendants urge us, in the alternative, to hold that the complaint fails to state a claim for which relief can be granted. See [Fed. R. Civ. P. 12\(b\)\(6\)](#). The district court did not reach the arguments defendants raised in their [Rule 12\(b\)\(6\)](#) motion. We decline to consider them for the first time on appeal and remand for consideration by the district court in the first instance. See [ABF Freight Sys., Inc. v. Int’l Bhd. of Teamsters](#), 645 F.3d 954, 965 (8th Cir. 2011).

End of Document

© 2017 Thomson Reuters. No claim to original U.S. Government Works.