APPEAL NOS. 16-2378, 16-2528

UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

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

Appeal from Judgment of the United States District Court for the District of Minnesota in Civil Action No. 14-md-2586 (Montgomery, J.)

BRIEF OF PLAINTIFFS-APPELLANTS MELISSA ALLERUZZO, ET AL

BARNOW AND ASSOCIATES, P.C.
Ben Barnow
One N. LaSalle Street, Ste. 4600
Chicago, IL 60602
(312) 621-2000 (p)
(312) 641-5504 (f)
b.barnow@barnowlaw.com

Additional Attorneys
Listed on Inside Page

Attorneys for Appellants

CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
Edwin J. Kilpela, Jr.
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15212
(412) 322-9243 (p)
(412) 231-0246 (f)
ekilpela@carlsonlynch.com

LAW OFFICE OF ARON D. ROBINSON
Aron D. Robinson
180 West Washington St., Suite 700
Chicago, IL 60602
(312) 857-9050 (p)
Adroblaw@aol.com

MCSWEENEY/LANGEVIN, LLC
Rhett A McSweeney
David M. Langevin
2116 2nd Avenue South
Minneapolis, Minnesota 55404
(612) 746-4646 (p)
(612) 454-2678 (f)
ram@westrikeback.com

THE DRISCOLL FIRM, P.C.
John J. Driscoll
Christopher J. Quinn
211 N. Broadway, 40th Floor
St. Louis, MO 63102
(314) 932-3232 (p)
john@thedriscollfirm.com
chris@thedriscollfirm.com

LOCKRIDGE GRINDAL NAUEN PLLP
Karen H. Riebel
100 Washington Avenue South,
Suite 2200
Minneapolis, MN 55401
(612) 339-6900 (p)
(612) 339-0981 (f)
khriebel@locklaw.com

STEWARD LAW FIRM, LLC
John S. Steward
1717 Park Avenue
St. Louis, Missouri 63104
(314) 571-7134 (p)
(314) 594-5950 (f)
Glaw123@aol.com

THE COFFMAN LAW FIRM
Richard L. Coffman
505 Orleans St., Suite 505
Beaumont, TX 77701
(409) 833-7700 (p)
(866) 835-8250 (f)
rcoffman@coffmanlawfirm.com

Attorneys for Appellants

SUMMARY OF THE CASE

This case concerns a data breach and subsequent disclosure of personal identifying information of Plaintiffs and the Class. The central issue pending before this Court is whether the named Plaintiffs have standing under Article III to bring suit against Defendants SuperValu, AB Acquisition, LLC, and New Albertsons, Inc., as a result of the data breach and disclosure. All Plaintiffs claim standing on account of the theft of their personal identifying information and the resultant substantial risk of suffering identity fraud and theft, as well as the time, money, and efforts necessary to mitigate the ongoing risk of fraud and identity theft. In addition, all Plaintiffs claim standing because Defendants, by failing to employ measures to adequately protect Plaintiffs' personal identifying information, breached implied contractual terms that accompanied each Plaintiff's purchases at Defendants' stores. Finally, Plaintiff Holmes also asserts standing due to the financial harm he suffered as a result of the data breach. The district court below erred when it dismissed Plaintiffs' claims for lack of Article III standing.

Oral argument is appropriate in this matter because the question of whether a plaintiff victimized by a data breach has standing to seek relief for the theft of their personal information, and the attendant harm that results from this theft, is a matter of first impression in this Court, and also is an open question in courts throughout the country. Appellants respectfully request 30 minutes of oral argument.

TABLE OF CONTENTS

Summary of the Case i

Table of Contents ii

Table of Authorities iii

Jurisdictional Statement 1

Statement of Issues 2

Statement of the Case 4

A. Statement of Facts 4

B. Relevant Procedural History 7

C. Rulings Presented for Review 8

Summary of Argument 9

Argument 13

A. Standard of Review and Legal Standard 13

B. The Theft of Plaintiffs' PII Constitutes an Article III Injury-in-Fact 15

C. The Fraudulent Charge Suffered by Plaintiff Holmes is Fairly Traceable to the Data Breach 27

D. Defendants' Breach of the Implied Contract Terms Confers Standing 31

Conclusion 33

TABLE OF AUTHORITIES

Page(s)

Cases

ABF Freight Sys., Inc. v. Int'l Bhd. of Teamsters,
645 F.3d 954 (8th Cir. 2011) 13, 32

Anderson v. Hannaford Bros. Co.,
659 F.3d 151 (1st Cir. 2011).....19

In re Barnes & Noble Pin Pad Litig. ("B&N"),
No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) 28, 29

Biscanin v. Merrill Lynch & Co.,
407 F.3d 905 (8th Cir. 2005) 13, 21

Branson Label, Inc. v. City of Branson, Mo.,
793 F.3d 910 (8th Cir. 2015) 13

Brown v. Town & Country Masonry & Tuckpointing, LLC,
No. 4:12-CV-1227-DDN, 2012 WL 6013215 (E.D. Mo. Dec. 3,
2012) 33

Clapper v. Amnesty Int'l USA,
133 S. Ct. 1138 (2013).....15, 18

Coccoli v. Daprato,
No. CIV.A. 13-12757-MBB, 2014 WL 1908934 (D. Mass. May
12, 2014) 32

E-shops Corp. v. U.S. Bank Nat'l Ass'n,
678 F.3d 659 (8th Cir. 2012) 30

Krottner v. Starbucks Corp.,
628 F.3d 1139 (9th Cir. 2010) 16, 23

Lewert v. P.F. Chang's China Bistro, Inc.,
819 F.3d 963 (7th Cir. 2016) .....*passim*

Katz v. Pershing, LLC,
672 F.3d 64 (1st Cir. 2012).....3, 31, 32

Spokeo, Inc. v. Robins,
136 S. Ct. 1540 (2016).....*passim*

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992).....13,14, 21

In re Nickelodeon Privacy Litig.,
___ F.3d ___, 2016 WL 3513782 (3d Cir. June 27, 2016).....25, 26

Pisciotta v. Old. Nat'l Bancorp,
499 F.3d 629 (7th Cir. 2007) 24

Remijas v. Neiman Marcus Group, LLC,
794 F.3d 688 (7th Cir. 2015) .....*passim*

Resnick v. AvMed, Inc.,
693 F.3d 1317 (11th Cir. 2012) 3, 27, 28, 29

Salve Regina Coll. v. Russell,
499 U.S. 225 (1991).....13

So. Shore Hellenic Church, Inc. v. Artech Church Interiors, Inc.,
No. 12-11663, 2015 WL 846533 (D. Mass. Feb. 25, 2015).....32

In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,
996 F. Supp. 2d 942 (S.D. Cal. 2014).....16

Susan B. Anthony List v. Driehaus,
134 S. Ct. 2334 (2014).....14, 15, 23, 27

Sutton v. St. Jude Med. S.C. Inc.,
419 F.3d 568 (6th Cir. 2005) 25

In re Target Corp. Data Sec. Breach Litig.,
66 F. Supp. 3d 1154 (D. Minn. 2014).....3, 27

Statutes

28 U.S.C. § 1291 1

28 U.S.C. § 1332(d)(2).....1

Other Authorities

Charles Alan Wright, Arthur R. Miller, Mary Kay Kane, Fed. Prac. & Proc. Civ. 3d § 1785.1 (2005) 15, 16

Federal Rule of Appellate Procedure 4(a)(4)(iv) 1

Federal Rule of Civil Procedure 12 ..... 12, 13

Federal Rule of Civil Procedure 59(e) 1

Merriam-Webster's Online Dictionary, Definition of "Risk," http://www.merriam-webster.com/dictionary/risk (last visited June 22, 2016) 22

U.S. Const., Art. III ..... *passim*

JURISDICTIONAL STATEMENT

The district court had jurisdiction under 28 U.S.C. § 1332(d)(2) because Plaintiffs-Appellants' Amended Class Action Complaint ("CAC") alleges claims on behalf of Plaintiffs and other class members that exceed $5,000,000, exclusive of interests and costs, and there are numerous class members who are citizens of states other than Defendants-Appellees' states of citizenship. JA-15; CAC ¶ 14.[1]

This Court has jurisdiction under 28 U.S.C. § 1291 because Plaintiffs timely appealed a final order. Twenty-eight days after the district court entered judgment dismissing Plaintiffs' CAC, JA-131, Plaintiffs filed a motion to alter or amend pursuant to Federal Rule of Civil Procedure 59(e), JA-132, which the district court denied, JA-227. Twenty-eight days after that denial, Plaintiffs filed their notice of appeal, seeking review of the district court's judgment dismissing Plaintiffs' CAC. JA-235. Defendants subsequently filed a notice of cross appeal. JA-243. As Plaintiffs filed their notice within thirty days of the district court's denial of their motion to alter or amend, this appeal is timely under Federal Rule of Appellate Procedure 4(a)(4)(iv).

---

[1] All references to the joint appendix filed contemporaneously herewith and referenced herein are abbreviated as "JA-" followed by the page number(s). Plaintiffs' CAC begins at JA-12 and is referred to throughout as "CAC" followed by the relevant paragraph(s). All references to Plaintiffs' addendum filed contemporaneously herewith and referenced herein are abbreviated as "ADD-" followed by the page number(s).

STATEMENT OF ISSUES

1. Does a consumer have Article III standing based on the substantial and imminent risk of harm that occurs when a consumer's personal identifying information is taken by a criminal intrusion into a retailer's point-of-sale computer network, it is well-known that substantially similar data breaches have resulted in substantial harm to consumers in identity-fraud and identity-theft-related losses, and evidence obtained from payment card issuing financial institutions evinces significant fraud on cards compromised by the data breach?

List of Apposite Cases: *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966 (7th Cir. 2016); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692-96 (7th Cir. 2015).

Most Apposite Constitutional Provision: U.S. Const., Art. III.

2. Is a consumer's harm fairly traceable to a data breach where the consumer notices a fraudulent charge on the consumer's credit card account shortly after the data breach and thus sufficient to confer Article III subject matter jurisdiction on a federal court over the consumer's claims against the breached retailer?

List of Apposite Cases: *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154 (D. Minn. 2014); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012).

Most Apposite Constitutional Provision: U.S. Const., Art. III.

3. Does a consumer have Article III standing to enforce an alleged implied contractual agreement between the consumer and a payment card accepting merchant to exercise reasonable care and observe industry standard security measures with respect to the storage, transmission, and use of the consumer's payment card data?

List of Apposite Cases: *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012).

Most Apposite Constitutional Provision: U.S. Const., Art. III.

STATEMENT OF THE CASE

A. Statement of Facts

This appeal concerns whether Plaintiffs-Appellants 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, and Darla Young (collectively, "Plaintiffs") have standing to assert claims for the theft of their personal financial and identifying information, including, but not limited to their names, account numbers, card expiration dates, PINs, and other numerical information (collectively, "Personal Identifying Information" or "PII"), which was stolen in a 2014 breach of SuperValu's point-of-sale, payment card network (hereinafter "POS Network"). CAC ¶ 1. Appellee SuperValu, Inc. ("SuperValu") owns and operates regional grocery stores under various brand names and controls the payment processing services for those stores, as well as various other name-brand grocery stores owned and operated by Appellees AB Acquisition, LLC ("AB Acquisition") and New Albertson's, Inc. ("Albertson's") (collectively, "Defendants"). CAC ¶¶ 2–3, 33–35.

Between at least June 22, 2014, and July 17, 2014, hackers accessed and installed malicious software on SuperValu's POS Network. CAC ¶¶ 4–5, 36. The hackers, taking advantage of SuperValu's sub-standard security procedures, gained

access to the POS Network through remote access points. CAC ¶ 38. While inside SuperValu's POS Network, hackers were able to steal Plaintiffs' PII through the use of two techniques. First, the hackers installed RAM scraper malware to SuperValu's POS terminals. CAC ¶ 40. This malware harvested unencrypted payment card data and transmitted it to the hackers. CAC ¶ 40. Second, hackers directly accessed and stole consumer information that was stored improperly on SuperValu's POS Network. CAC ¶ 41. Hackers again gained access to SuperValu's POS Network between late August and early September 2014 (this intrusion and the June 22, 2014, through July 17, 2014, intrusion are collectively referred to as the "Data Breach"). CAC ¶¶ 6, 44. They again installed malware in the portion of SuperValu's POS Network that processes payment card transactions. CAC ¶ 44. The Data Breach affected over 1,000 SuperValu and AB Acquisition/Albertson's stores, CAC ¶¶ 4–5, 36, and resulted in the theft and misuse of the PII of Plaintiffs and members of the class, CAC ¶¶ 8–9.

After the Data Breach, Defendants offered Plaintiffs and all individuals affected by the Data Breach one year of free credit monitoring. CAC ¶ 45. This offer, however, was, and is, inadequate due to the nature of the data that was stolen, the protracted timeframe under which data theft victims potentially can suffer harm, and the failure to compensate for damages that also routinely occur with these breaches. Due to the extended usefulness of stolen PII, it often is used

long after a breach has occurred, and it can take some time for data theft victims to recognize that identity fraud has occurred. CAC ¶¶ 60, 72–76. Additionally, because the account information of consumers is less secure after theft of their PII, they reasonably take precautions, and spend additional time and money, to ensure that their personal and financial accounts are secure. CAC ¶ 78.

As with other publicized data breaches of major retailers, payment card issuers noticed a pattern of fraud on compromised cards after the Data Breach. One such financial institution received notification from Visa's Compromised Account Management System ("CAMS") that 272 cards it issued were placed at risk of fraud in the Data Breach. As of February 4, 2016, fifty-eight of these card accounts experienced actual instances of fraud, totaling $13,503.12. ADD-20; JA-226. Another issuer has observed fraud on five of 313 cards included on a Visa CAMS alert totaling $4,258.25 as of March 3, 2016. ADD-25. A third issuer reported on February 24, 2016, fraud on two out of three cards compromised in the Data Breach totaling $269.46. ADD-23.

Plaintiffs have been harmed through the theft of their personal information. For example, Plaintiff David Holmes noticed a fraudulent charge on his credit card shortly after the Data Breach. CAC ¶ 31. He promptly cancelled his card, and waited two weeks for a replacement card. CAC ¶ 31. Plaintiff Kenneth Hanff closed his checking account after the Data Breach and opened a new one to prevent

fraudulent charges. CAC ¶ 18. Furthermore, all Plaintiffs have had their PII stolen, and, as a result, are at an increased and imminent risk of suffering identity fraud, and have lost time and money monitoring their accounts in order to ensure that fraud does not occur. CAC ¶¶ 16–31. Finally, when Plaintiffs shopped at the stores owned and operated by Defendants, Defendants offered Plaintiffs the option to use their payment cards to purchase goods from Defendants. CAC ¶ 137. An implied contract term of this offer was that Defendants would take reasonable steps to safeguard the PII stored on Plaintiffs' payment cards. CAC ¶ 138. Indeed, had such a term not existed, Plaintiffs, as with other reasonable consumers, would not have used their cards to purchase goods in the first place. CAC ¶ 139. Plaintiffs accepted Defendants' offer when they used their payment cards to purchase products from Defendants, and fully performed their obligations under the contract. CAC ¶¶ 137, 140. Defendants, however, breached their duty under the contract and failed to take reasonable steps to protect Plaintiffs' PII. CAC ¶ 141. This breach harmed Plaintiffs, and took from them a right to which they were entitled under the implied contract.

B. Relevant Procedural History

Following the Data Breach, four putative class actions, consisting of twelve named plaintiffs, were filed against Defendants in Illinois, Minnesota, and Idaho. On December 16, 2014, the Judicial Panel on Multidistrict Litigation transferred

and centralized the cases in the United States District Court for the District of Minnesota. JA-9.

On June 26, 2015, Plaintiffs filed their CAC, which added four named plaintiffs in addition to the original twelve. JA-12. On August 10, 2015, Defendants filed a motion to dismiss, which, among other things, sought to dismiss the CAC for lack of Article III standing. JA-55. On January 7, 2016, the district court granted Defendants' motion, and dismissed the CAC for lack of subject-matter jurisdiction. ADD-1, 17. The district court entered judgment the same day. JA-131. On February 4, 2016, Plaintiffs filed a motion to alter or amend the judgment. JA-132. The district court denied Plaintiffs' motion on April 20, 2016. JA-227.

On May 28, 2016, Plaintiffs filed a notice of appeal, seeking review of the district court's January 7, 2016, judgment dismissing the CAC. JA-235. On May 31, 2016, Defendants' filed a notice of cross appeal. JA-243.

C. Rulings Presented For Review

Plaintiffs seek review of the district court's order, and the resulting judgment entered, granting Defendants' motion to dismiss and dismissing Plaintiffs' CAC for lack of subject matter jurisdiction. ADD-1; JA-131.

SUMMARY OF ARGUMENT

Plaintiffs have standing to bring this suit. The district court incorrectly dismissed for three primary reasons. First, the district court held that Plaintiffs had not adequately alleged the theft of their personal information, and that theft alone is insufficient to confer Article III standing. Second, the district court held that Plaintiff Holmes did not have standing—despite the fact that he alleged misuse of his personal information—because, according to the district court, that misuse was not fairly traceable to the Data Breach. Finally, the district court held that the breach of Plaintiffs' implied contractual right to have their PII securely handled and reasonably protected was not sufficient to confer standing. All of these holdings were erroneous.

Plaintiffs adequately alleged that their PII was stolen, and this theft is sufficient to establish injury-in-fact and confer standing. Defendants, entities who were entrusted with Plaintiffs' sensitive and valuable PII, and whose negligence in protecting that information was known to cause and would necessarily cause consumers serious and permanent harm, failed to adopt adequate and reasonable procedures to protect that information. Defendants' inaction permitted hackers to access Defendants' POS Network, install malicious software, and steal Plaintiffs' PII. In similar cases, many district courts and courts of appeals have held that victims of similar data breaches have standing to seek redress for their injuries

given the valuable nature of the information stolen and the ongoing risk of harm associated with its theft. Here, the operative complaint alleges that all Plaintiffs face a substantial risk of harm as a result of the theft of their PII. Indeed, Plaintiffs alleged in detail how their PII was stolen and how Defendants' failures enabled that theft. Numerous other breaches preceding this Data Breach teach by experience that the harm was (and is) real and certainly imminent within standing requirements. Moreover, the operative complaint points to evidence of misuse of Plaintiffs' PII, further buttressing the conclusion that Plaintiffs' PII was stolen and that the threat of harm is real and certainly impending.

Under well-established principles of standing—supported by several recent opinions in factually analogous cases—Plaintiffs' allegations of theft demonstrate injury-in-fact and are sufficient to confer standing. Indeed, the Supreme Court recently confirmed that a risk of real harm can suffice to establish injury-in-fact and has time and again affirmed that such a risk need not be literally certain. If, instead, allegations of identity theft and identity fraud are required, as the district court held, the substantial risk standard is rendered meaningless. The Seventh Circuit Court of Appeals, the Ninth Circuit Court of Appeals, and district courts around the country have recognized this proposition. Most notably, and in two recent opinions almost identical to the case at bar, the Seventh Circuit has held that the risk of future identity fraud and theft attendant to a data breach is sufficiently

concrete to qualify as Article III an injury-in-fact. This Court should reverse the district court and establish a similar rule in this jurisdiction.

In holding that the Plaintiffs lacked standing, the district court disregarded the allegations in the operative complaint and, instead, improperly weighed outside evidence and determined unilaterally that Plaintiffs' information was not stolen. The court then concluded that Plaintiffs and the Class are not at any risk of future harm. Specifically, the district court gave substantial weight to press releases issued by Defendants, which stated that Plaintiffs' PII was not stolen, and devalued or discounted Plaintiffs' specific allegations of theft, holding that Plaintiffs' allegations of theft were not credible because Plaintiffs failed to allege widespread misuse. This ruling was erroneous for several reasons. Plaintiffs plainly alleged that their PII was stolen, regardless of what Defendants have said in unexamined and unchallenged press releases that have not been subject to scrutiny during the discovery process. Furthermore, the district court's ruling stands both the pleading rights of plaintiffs, in this case and others, and the discovery process, on their heads and requires Plaintiffs to obtain evidence that would in most cases only be available during discovery—and certainly not in a case where discovery has been greatly restricted, as was done here.

The district court's ruling denying standing is also directly contrary to the experience of Plaintiff Holmes, who specifically alleged that his PII was misused

and that he incurred financial harm as a result. The district court discounted Mr. Holmes injury, however, holding that it was not fairly traceable to the Data Breach because Mr. Holmes was the only named Plaintiff to have alleged fraudulent charges on a payment card. This conclusion was mistaken because Mr. Holmes alleged that his PII was misused a short time after the occurrence of the Data Breach and, that, at the pleading stage, was adequate. Plaintiff Holmes need not establish class-wide standing for his fraud charge or rule out all other possible causes for his fraud charge. Such determinations are appropriate at the class certification stage when such issues can be evaluated with the benefit of discovery. The district court's holding to the contrary was mistaken and should be reversed.

Finally, all Plaintiffs have standing because Plaintiffs alleged that Defendants' conduct constitutes a breach of an implied contractual term. No reasonable person, Plaintiffs included, would use their debit- or credit-card at a retailer if they knew that retailer would fail to safeguard its data systems permitting the theft of their PII. Therefore, an implied contract was created between retailer and customer requiring the retailer to adopt reasonable procedures to protect Plaintiffs' PII. Defendants breached this contractual term through their failure to adequately and reasonably protect Plaintiffs' PII. The breach of that implied contract is yet another legally protected right sufficient to confer Plaintiffs standing and the district court's failure to recognize this injury was erroneous.

ARGUMENT

A. Standard of Review and Legal Standard

This appeal concerns the district court's dismissal of Plaintiffs' CAC for lack of subject-matter jurisdiction pursuant to Fed. R. Civ. P. 12(b)(1). ADD-1; JA-131. "The existence of subject-matter jurisdiction is a question of law that . . . [is] review[ed] de novo." *ABF Freight Sys., Inc. v. Int'l Bhd. of Teamsters*, 645 F.3d 954, 958 (8th Cir. 2011). "When *de novo* review is compelled, no form of appellate deference is acceptable." *Salve Regina Coll. v. Russell*, 499 U.S. 225, 238 (1991).

Where, as here, a defendant makes a "facial attack" to the subject matter jurisdiction of a plaintiff's complaint, "the court restricts itself to the face of the pleadings, and the non-moving party receives the same protections as it would defending against a motion brought under Rule 12(b)(6)." *Branson Label, Inc. v. City of Branson, Mo.*, 793 F.3d 910, 914 (8th Cir. 2015) (quoting *Osborn v. U.S.*, 918 F.3d 724, 729 n.6 (8th Cir. 1990)) (quotation marks omitted). In other words, the court must, based on the allegations contained in the plaintiff's complaint, "draw[] all reasonable inferences in favor of the plaintiff," and determine whether the plaintiff has adequately alleged all elements necessary for subject matter jurisdiction. *Biscanin v. Merrill Lynch & Co.*, 407 F.3d 905, 907 (8th Cir. 2005); *see Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) ("At the pleading

stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss [courts] 'presume that general allegations embrace those specific facts that are necessary to support the claim.'" (internal citation omitted).

To have Article III standing, a plaintiff must show "(1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Lujan*, 504 U.S. at 560–61) (quotation marks and alterations omitted). Although the "party invoking federal jurisdiction bears the burden of establishing standing . . . , [e]ach element must be supported . . . [only to] the manner and degree [] required at the successive stages of the litigation." *Id.* at 2342.

Here, Plaintiffs have established Article III standing. First, all Plaintiffs have standing because the theft of their PII has put them at a substantial risk of suffering identity theft and fraud. Second, Plaintiff Holmes has standing because, in addition to his substantial risk of identity theft and fraud, the fraudulent credit card charge he suffered is fairly traceable to Defendants' failure to secure his PII. Finally, all Plaintiffs have standing because Defendants' breach of an implied contract term has denied them a contractual right to which they are entitled. For all of these reasons, the district court erred in finding Plaintiffs lacked standing, and

its judgment dismissing the CAC should be reversed and this case remanded for further proceedings.

B. The Theft of Plaintiffs' PII Constitutes an Article III Injury-In-Fact

"To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (internal citations omitted). To be "particularized," an injury-in-fact "must affect the plaintiff in a personal and individual way." *Id.* To be "concrete," an injury-in-fact "must be 'de facto'; that is, it must actually exist"—it must be "'real,' and not 'abstract.'" *Id.* (internal citations omitted). "'Concrete' is not, however, necessarily synonymous with 'tangible.' Although tangible injuries are perhaps easier to recognize . . . intangible injuries can nevertheless be concrete." *Id.* at 1549 (internal citations omitted). Importantly, "[t]his does not mean, however, that the risk of real harm cannot satisfy that requirement." *Id.* And in assessing risk, that risk need not be "literally certain." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1150 n.5 (2013); *see also Driehaus*, 134 S. Ct. at 2431 ("An allegation of future injury may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.") (quotation marks omitted); Charles Alan Wright, Arthur R. Miller, Mary Kay Kane, Fed. Prac. & Proc. Civ. 3d § 1785.1 (2005) ("If [a] plaintiff can

show that there is a possibility that [the] defendant's conduct may have a future effect, even if injury has not yet occurred, the court may hold that standing has been satisfied.").

Other courts of appeals have determined that the risk of real harm, in the form of identity fraud and theft, suffered by plaintiffs whose personal information is stolen by hackers, is "the type of 'certainly impending' future harm that the Supreme Court requires to establish [injury-in-fact]." *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966 (7th Cir. 2016) (finding injury-in-fact based on allegations of theft of the plaintiffs' personal information) (internal citation omitted); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692–96 (7th Cir. 2015) (same); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141–43 (9th Cir. 2010) (same); *see also In re Adobe Sys. Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1212–16 (N.D. Cal. 2014) (same); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014) (same). This Court should adopt the reasoning of *Lewert*, *Remijas*, and *Krottner*, and conclude the same.

In *Lewert v. P.F. Chang's*, the defendant announced that its computer system had been breached and that consumer credit- and debit-card data had been stolen from all of its stores. 819 F.3d at 965. The defendant later contended that only thirty-three restaurants had been affected. *Id.* While neither of the named

plaintiffs dined at any of the thirty-three restaurants the defendant unilaterally determined were affected, one plaintiff noticed fraudulent charges on his card after the breach, and both plaintiffs monitored their accounts for fraudulent activity. *Id.*

The Seventh Circuit held that the plaintiffs had standing to bring suit because their card data had *already* been stolen. *Id.* at 966–69. The theft of this data made it "plausible to infer a substantial risk of future harm . . . because a primary incentive for hackers is 'sooner or later to make fraudulent charges or assume those consumers' identities.'" *Id.* at 967 (quoting *Remijas*, 794 F.3d at 693). The court further held that P.F. Chang's contention that the plaintiffs' data was not stolen "create[d] a factual dispute about the scope of the breach, but d[id] not destroy standing." *Id.* at 968. While P.F. Chang's would be afforded the opportunity to argue that the plaintiffs' data was not stolen, that determination was better left for the merits. *Id.*

Here, as in *Lewert*, Plaintiffs have suffered an Article III injury-in-fact because their PII has already been stolen. CAC ¶¶ 8–9. Not only did Plaintiffs allege that hackers were able to gain access to their PII, they also have alleged the mechanism through which the hackers were able to steal that information. *See* CAC ¶¶ 38–41. Specifically, Plaintiffs alleged that hackers installed malware, undetected for weeks, that captured unencrypted PII from POS devices on SuperValu's POS Network and then transmitted that information to the hackers,

and that hackers were able to steal Plaintiffs' PII because that information was stored improperly by SuperValu on its POS Network. CAC ¶¶ 40–41. This is the same or a similar method used in other notorious data breaches that have resulted in substantial harm to consumers and about which retailers have been warned by Visa. CAC ¶¶ 48, 58; ADD-18–25; JA-224. Further, Plaintiff Holmes suffered a fraudulent charge shortly after SuperValu's POS Network was breached, a temporal connection that suggests that consumer PII was stolen during the Data Breach. CAC ¶ 31. As in *Lewert*, the theft of Plaintiffs' PII makes it plausible to infer a substantial risk of future harm because the primary incentive for the hackers who stole that information is to misuse it for financial gain.

Because the theft of Plaintiffs' PII puts Plaintiffs at a substantial risk of suffering future harm, the costs they must incur to mitigate that risk, including the time and money spent protecting themselves from potential identity theft and fraud, CAC ¶¶ 16–31, should also grant them Article III standing. *See Clapper*, 133 S. Ct. at 1150 n.5 & 1151 (recognizing that plaintiffs cannot manufacture standing "merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending" but also holding that if the future harm being mitigated is itself imminent or there is a substantial risk it will occur, costs incurred in an effort to mitigate the risk constitute an injury-in-fact); *Remijas*, 794 F.3d at 693–94 (applying *Clapper* to hold that "a substantial

risk of harm from the Neiman Marcus data breach" constituted an imminent harm such that mitigation expenses constituted a "concrete injury"); *Adobe*, 66 F. Supp. 3d at 1217; *cf. Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 162–65 (1st Cir. 2011) (before *Clapper*, holding that mitigation damages constitute injury-in-fact and recoverable damages in the context of a data breach as long as they were reasonable at the time, regardless of whether they end up being necessary in hindsight).

The district court failed to apply the proper standard of review because it did not accept the facts Plaintiffs alleged as true and failed to make all reasonable inferences in their favor. Instead, the district court engaged in improper fact-finding and weighing of evidence, and, disregarding the burden of proof and its role at the motion to dismiss stage, disbelieved Plaintiffs' allegations of theft. The district court stated that Plaintiffs' allegations of theft were based on Defendants' press releases, which stated that "there [was] no determination that customer data was stolen by the [hackers]." ADD-10–11 n.2. Because the press releases only stated that the data was accessed, the district court ignored Plaintiffs' allegations of theft, which the district court determined relied on Defendants' press releases for their validity. ADD-10–11 n.2. This holding was incorrect. And, of course, the district court disregarded the information Plaintiffs later obtained, despite restricted discovery, confirming misuse and related theft. *See* ADD-18–25; JA- JA-147–226.

Although Plaintiffs cited Defendants' press releases, they also explained how hackers gained access to SuperValu's POS Network, CAC ¶ 38, and explained the malware and techniques the hackers used to exfiltrate data from the POS Network. CAC ¶¶ 40–42. These allegations, standing alone, make it more than plausible that Plaintiffs' PII was stolen.

Even if Plaintiffs alleged only that hackers gained access to their PII, the risk of harm nevertheless is impending and substantial. It is unreasonable to infer that data thieves risked long prison terms to access large volumes of private consumer information but did not intend to use that information for any untoward purpose, such as identity theft or financial fraud. Moreover, the idea that the RAM scraper malware installed on SuperValu's POS Network only captured consumer data, but did not transmit that data to the hackers who installed the malicious software, is untenable. First, it is at least plausible that Plaintiffs' allegations that it was transmitted are true. Second, Plaintiff Holmes' allegations of a contemporaneous fraudulent charge provide a plausible inference that Plaintiffs' PII actually was transmitted. It is true that Defendants contest whether Plaintiffs' PII was stolen. "This creates a factual dispute about the scope of the breach, but it does not destroy standing." *Lewert*, 819 F.3d at 968. The district court erred by failing to take Plaintiffs' allegations as true, and by failing to make all reasonable inferences in their favor.

In addition to disregarding Plaintiffs' well-pled allegations, the district court erroneously held that without allegations of widespread data misuse, Plaintiffs' risk of future harm was too speculative to constitute an Article III injury-in-fact. ADD-9. Absent such allegations, the district court determined that it was "left to speculate about whether the hackers who gained access to Defendants' payment processing network were able to capture or steal Plaintiffs' PII; whether the hackers or other criminals will attempt to use the PII; and whether those attempts will be successful." ADD-10–11. The district court's conclusions are mistaken under both Supreme Court precedent and analysis adopted by other circuit courts of appeals.

Had the district court taken Plaintiffs' allegations as true, as required, no speculation would be necessary. Plaintiffs alleged that their information was stolen, and explained in detail how the data theft occurred. CAC ¶¶ 8–9, 38–42. It is clear that the district court disbelieved these fact allegations when it speculated about whether hackers "were able to capture or steal Plaintiffs' PII." ADD-10. But on a facial challenge to subject matter jurisdiction, the district court was required both to "draw[] all reasonable inferences in favor of the plaintiff," *Biscanin*, 407 F.3d at 907, and also to "presume that general allegations embrace those specific facts that are necessary to support the claim," *Lujan*, 504 U.S. at 561 (internal quotation marks omitted). Plaintiffs went beyond the standard

required by *Lujan* and alleged not only general facts and allegations that their PII was compromised but also provided a concrete mechanism through which the theft occurred. Furthermore, the theft of Plaintiffs' PII leads to the reasonable inference that the hackers who stole it intend to, and are capable of, misusing that information: why else would hackers break into a store's database, run the risk of significant jail time, and steal consumer PII unless they intended to, and were capable of, misusing that information for illicit gain? The purpose of hacking consumer information, such as the treasure trove of PII compromised in the Data Breach, is to facilitate identity theft and financial fraud. *Accord Remijas*, 794 F.3d at 693. Accordingly, had the district court properly analyzed Plaintiffs' allegations and taken them as true, any speculation regarding their increased risk of future injury was unnecessary.

In reaching its conclusions, the district court also held that Plaintiffs' increased risk of harm was speculative because the court could not determine "when" any future injury would occur. ADD-9, 11. But the fact that Plaintiffs cannot precisely determine when their harm will occur, does not, in itself, preclude standing. In fact, the long-standing threat that at any moment they may suffer harm makes the risk all the more real and substantial. As argued earlier, *Spokeo* makes clear that "the *risk* of real harm" can satisfy Article III's injury-in-fact requirement. 136 S. Ct. at 1549 (emphasis added). A "risk" is defined as "the

possibility that something . . . will happen." *See* Merriam-Webster's Online Dictionary, Definition of "Risk," http://www.merriam-webster.com/dictionary/risk (last visited June 22, 2016). A "risk" involves the "possibility," rather than the "certainty," of occurrence; thus, when a plaintiff relies on a risk of real harm to establish injury-in-fact, she or he necessarily is relying on a possibility of future harm to establish standing. What matters is that the possibility is "certainly impending" or "substantial." *See Driehaus*, 134 S. Ct. at 2341.

The risk that Plaintiffs will suffer future harm is both certainly impending and substantial. Their PII is in the hands of hackers who specifically targeted that information and have the requisite skill and intent to use that information for nefarious and illegal purposes. As a result, the mere fact that Plaintiffs cannot pinpoint when their harm will occur makes the risk more substantial and imminent.

In supporting its holding, the district court cited *Reilly v. Ceridian Corp.*, which is not only distinguishable but also wrongly decided. 664 F.3d 38 (3d Cir. 2011). In *Reilly*, the plaintiffs alleged that hackers infiltrated the defendant's data system and *potentially* gained access to the plaintiffs' personal information and the personal information of approximately 27,000 employees of various companies. 664 F.3d at 40. The plaintiffs *did not* allege that the hacker read, copied, or understood the data. *Id.* In fact, taking the plaintiffs' allegations as true, the Third Circuit could only infer that "a firewall was penetrated." *Id.* at 44. The court

distinguished the Ninth Circuit's decision in *Krottner* and the Seventh Circuit's decision in *Pisciotta v. Old. Nat'l Bancorp*, 499 F.3d 629, 632 (7th Cir. 2007), on the basis that "[h]ere, there is no evidence that the intrusion was intentional or malicious." *Reilly*, 664 F.3d at 44. The court also emphasized that the "Plaintiffs have alleged no misuse." *Id.*

The plaintiffs in *Reilly* were found to not have standing because their Article III injury-in-fact (*i.e.*, their increased risk of future identity fraud) was based on something that may not have happened. The plaintiffs did not allege that the hacker stole, or was in possession of, their personal information, but rather, based on the fact that the defendant's data systems had been breached, speculated that theft had occurred. *Id*. at 42–46. The *Reilly* plaintiffs lacked standing as a result of this pleading deficiency because the court was unable to determine that the plaintiffs' data "ha[d] been—or w[ould] ever be—misused." *Id.* at 43. In support of its holding, the court emphasized that "a number of courts have had occasion to decide whether the 'risk of future harm' posed by data security breaches confers standing on persons whose information *may* have been accessed," and "[m]ost courts have held that such plaintiffs lack standing because the harm is too speculative." *Id.* (emphasis in original) (internal citations omitted).

Here, in contrast to *Reilly*, Plaintiffs have specifically alleged that their PII was stolen, and explained how that theft was perpetrated in a sophisticated,

intentional, and malicious way that has resulted in substantial harm to countless consumers in this and other data breaches. Plaintiffs have also alleged and shown subsequent misuse of the compromised PII of Mr. Holmes and other unnamed class members. These allegations clearly support the contention that Plaintiffs' information was stolen and that Plaintiffs are at an increased risk of fraud and identity theft as a result. Although Plaintiffs "may eventually not be able to provide an adequate factual basis for th[ese] inference[s], [] they ha[ve] no such burden at the pleading stage." *Remijas*, 794 F.3d at 694; *see also Lewert*, 819 F.3d at 968 ("The plaintiffs plausibly allege that their data was stolen . . . . This creates a factual dispute about the scope of the breach, but it does not destroy standing. P.F. Chang's will have the opportunity to present evidence to explain how the breach occurred and which stores it affected."); *Sutton v. St. Jude Med. S.C. Inc.*, 419 F.3d 568, 575 (6th Cir. 2005) (holding that a district court prematurely evaluated the merits of the plaintiff's claims and that "an increased risk of harm when comparing those individuals implanted with the [defective medical] device to those undergoing traditional surgery" was sufficient to establish standing at the pleading stage). Indeed, the Third Circuit recently held, post-*Spokeo*, that "the unlawful disclosure of legally protected information," on its own, constituted a sufficiently concrete harm for purposes of Article III standing, even though that

harm was intangible. *In re Nickelodeon Privacy Litig.*, ___ F.3d ___, 2016 WL 3513782, at *7–*8 (3d Cir. June 27, 2016).

Finally, requiring widespread misuse of PII in order to take as true allegations that the PII was stolen is fraught with problems. While corporate defendants have inside knowledge regarding the details and scope of data breaches, including what was stolen and who was affected, consumer plaintiffs only have knowledge concerning themselves and what they are told. Requiring data breach plaintiffs to allege facts that are in a defendant's exclusive possession, and only available through the discovery process, places an insurmountable burden on such plaintiffs. It also means that defendants can avoid liability simply by withholding relevant information from the public and hiding or denying the details of any data breach that has occurred. Allowing a defendant to control consumers' access to the federal courts by picking and choosing what information to admit and disclose is in fundamental opposition to the fact-finding function of the federal judicial system. And Plaintiffs believe that is what happened here. Declarations obtained by Plaintiffs cast grave doubt over Defendants' claims, under oath, that they lack knowledge of fraudulent activity. *See* ADD-18–25; JA-147–223. This evidence alone, in addition to the clear law cited by Plaintiffs, defeats the district court's reliance on Defendants' assertions of no such activity and the concomitant dismissal of the case.

In sum, the district court erred for all of the reasons contained herein, and its ruling should be reversed and this case remanded for further proceedings.

C. The Fraudulent Charge Suffered By Plaintiff Holmes Is Fairly Traceable to the Data Breach

In addition to establishing "injury-in-fact," a plaintiff also must show a sufficient causal connection between the harm suffered and the defendant's actions. *Driehaus*, 134 S. Ct. at 2341. Courts have routinely held that when plaintiffs allege that their data was stolen, and that they have suffered fraudulent charges, they have pled enough facts to raise the reasonable inference that their harm is fairly traceable to the data breach. *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327–28 (11th Cir. 2012) (finding two plaintiffs' identity fraud harms fairly traceable to theft of stolen laptop where plaintiffs alleged that information contained on the laptop was the same information used by hackers to occasion identity fraud, and plaintiffs alleged that identity fraud occurred ten and fourteen months after laptop theft); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1158–59 (D. Minn. 2014) (finding named plaintiffs' injuries, which included unauthorized charges, fairly traceable to data breach of the defendant's POS systems). The Court here should conclude the same.

Here, similar to the plaintiffs in *Target* and *Resnick*, Plaintiff Holmes alleged that his credit card information was stolen in the data breach, CAC ¶¶ 1, 8, 31, and that he incurred a fraudulent credit card charge shortly after the Data Breach, CAC

¶ 31. The fact that the sensitive information stolen during the breach was the same sensitive information used soon thereafter to incur fraudulent charges on Plaintiff Holmes' credit card account indicates a logical connection between the Data Breach and Mr. Holmes' financial harm. *See Resnick*, 693 F.3d at 1327 ("Plaintiffs allege a nexus between the two events that includes more than a coincidence of time and sequence: they allege that the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs' identity."). Plaintiff Holmes has plausibly alleged that his injury is fairly traceable to Defendants' actions, and he has standing as a result.

In comparison, the only case the district court cited in support in support of its holding on this issue, *In re Barnes & Noble Pin Pad Litig. ("B&N")*, No. 12-cv-8617, 2013 WL 4759588, at *6 (N.D. Ill. Sept. 3, 2013), is no longer good law under subsequently issued Seventh Circuit controlling authority.[2] While *B&N* held that it was not directly apparent that the *B&N* plaintiff's fraudulent charge was in any way related to the *B&N* defendant's data breach, that rationale does not survive the Seventh Circuit's decisions in *Remijas* and *Lewert*, discussed

[2] Plaintiffs in *B&N* have also filed an amended complaint that is awaiting a renewed motion to dismiss in light of *Remijas* and *Lewert*, which provides an additional indication that *B&N* should not have been relied upon by the district court, as the case in no way constitutes a final ruling. *See* First Am. Consolidated Class Action Compl., *B&N*, No. 12-cv-8617 (N.D. Ill. Sept. 24, 2013), ECF No. 58; Notice of Suppl. Authority in Supp. of Pls.' Opp'n to Barnes & Noble's Mot. to Dismiss the First Am. Consolidated Class Action Compl., *B&N*, No. 12-cv-8617 (N.D. Ill. Apr. 14, 2016), ECF No. 117.

extensively herein. In fact, in *Lewert*, nearly identical to the case at bar, the operative complaint alleged details of only a single fraudulent credit card charge. 819 F.3d at 965. Yet, the *Lewert* court still found a causal connection between the fraudulent charge and the *Lewert* defendant's data breach. *Id.* at 969. Accordingly, *B&N* is no longer good law, is not based on sound logic, and should not be followed. Rather, this Court should follow *Lewert* and *Resnick* and conclude that Plaintiff Holmes' allegations of causation are sufficient to survive a motion to dismiss.

The district court held that Plaintiff Holmes' fraudulent charge was not fairly traceable to the Data Breach because he was the only named plaintiff who alleged any sort of financial harm. ADD-3, 10. The district court noted that over 1,000 stores had been affected, but the only evidence of misuse was provided by Mr. Holmes, and stated that "[g]iven the unfortunate frequency of credit card fraud, it is common sense to expect that in any group similar in size to the sixteen Plaintiffs and multitudes of potential class members who used their payment cards at one of the 1,000-plus Affected Stores would likely experience at least one instance of a fraudulent charge." ADD-10. The district court's holding is mistaken on multiple levels.

First, the Supreme Court recently made clear that there is no threshold number of plaintiffs alleging an injury like that alleged by Plaintiff Holmes in

order to establish a causal connection. "That a suit may be a class action adds nothing to the question of standing, for even named plaintiffs who represent a class must allege and show that they personally have been injured, not that injury had been suffered by other, unidentified members of the class to which they belong." *Spokeo*, 136 S. Ct. at 1547 n.6 (internal alterations and quotes omitted). Plaintiff Holmes has alleged a plausible and causal connection between his injury and the Data Breach, and that is sufficient for purposes of Article III standing, regardless of injuries pled by any other plaintiff.

Additionally, at the motion to dismiss stage, it is enough to suggest a plausible, causal connection between the injury suffered and the harm suffered; plaintiffs need not plead facts from which all other possible causes of fraud could be ruled out. *See also E-shops Corp. v. U.S. Bank Nat'l Ass'n*, 678 F.3d 659 (8th Cir. 2012) (assuming without deciding that subject matter jurisdiction exists over controversy about fraudulent charges between online merchant and issuing bank that was allegedly breached, without requiring allegations that any other merchants complained of chargebacks). Whether it was ultimately Defendants' conduct, or the conduct of some other company, that caused Plaintiff Holmes' harm is not a question of standing, but rather, a theory of defense. "If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then 'the common law of torts has long shifted the burden of proof to

defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury.'" *Remijas*, 794 F.3d at 696 (quoting *Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J., concurring)); *see also Lewert*, 819 F.3d at 969 ("Merely identifying potential alternative causes does not defeat standing.").

Defendants certainly may argue that they did not cause Plaintiff Holmes' harm. But speculation by the district court that other unspecified occurrences may have been the actual cause of Holmes' harms does not undermine the plausibility of the inference that the Data Breach caused his harm. To accept a defendant's claim at this stage in that manner shuts out the light of justice on any dispute. That is not our judicial system. At this stage, Plaintiff Holmes' allegations that his information was stolen, and that shortly after that theft the same information was used to occasion identity fraud, are sufficient to establish standing. That is our judicial system. For this and each of the other reasons, the Court should reverse the district court's judgment and remand this case for further proceedings.

D. Defendants' Breach of the Implied Contract Terms Confers Standing

"The invasion of a common-law right (including a right conferred by contract) can constitute an injury sufficient to create standing." *Katz v. Pershing, LLC*, 672 F.3d 64, 72 (1st Cir. 2012) (citing *Ala. Power Co. v. Ickes*, 302 U.S. 464, 479 (1938)). "[W]hen a plaintiff generally alleges the existence of a contract,

express or implied, and a concomitant breach of that contract, her pleading adequately shows an injury to her rights." *Id.* This is consistent with Eighth Circuit precedent. *ABF Freight Sys., Inc. v. Int'l Bhd. of Teamsters*, 645 F.3d 954, 960–61 (8th Cir. 2011) (concluding Article III standing inquiry satisfied when breach of contract alleged).

Here, Plaintiffs have alleged the invasion of a right conferred by implied contract. Defendants offered Plaintiffs the option to use their payment cards to purchase goods from Defendants. CAC ¶ 137. Plaintiffs accepted that offer when they purchased goods from Defendants using their payment cards. CAC ¶¶ 137, 140. An implied contract term was that Defendants would take reasonable steps to safeguard Plaintiffs' PII contained on their payment cards. CAC ¶ 138. Indeed, had such a term not existed, Plaintiffs never would have used their cards to purchase goods from Defendants in the first place. CAC ¶ 139. As alleged in the complaint, Defendants breached this implied term by failing to take reasonable steps to protect Plaintiffs' PII. CAC ¶¶ 36–61. Accordingly, Plaintiffs have standing for this additional reason. *Accord So. Shore Hellenic Church, Inc. v. Artech Church Interiors, Inc.*, No. 12-11663, 2015 WL 846533, at *7, *9 (D. Mass. Feb. 25, 2015) (denying a motion to dismiss on standing grounds when alleging violation of a contractual right); *Coccoli v. Daprato*, No. CIV.A. 13-12757-MBB, 2014 WL 1908934, at *7–*8 (D. Mass. May 12, 2014) (same);

Brown v. Town & Country Masonry & Tuckpointing, LLC, No. 4:12-CV-1227-DDN, 2012 WL 6013215, at *6 (E.D. Mo. Dec. 3, 2012) (same).

The district court disregarded and misconstrued this injury. Specifically, the district court held that Plaintiffs failed to allege lost benefit of the bargain because they failed to allege that the value of the goods or services they purchased was diminished as a result of the Data Breach. ADD-16. Plaintiffs, however, never attempted to allege that the value of the goods or services purchased was diminished. Instead, as explained above, Plaintiffs argued that their contractual rights were violated. Accordingly, the district court's rationale is irrelevant because it failed to consider this additional basis for standing, and the court's judgment should be reversed.

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that this Court reverse the January 7, 2016, Order and Judgment of the district court and remand this case to the district court for further proceedings.

Dated: July 12, 2016

Respectfully submitted,

By: /s/ Ben Barnow

CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
Edwin J. Kilpela, Jr.
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15212
(412) 322-9243 (p)
(412) 231-0246 (f)
ekilpela@carlsonlynch.com

BARNOW AND ASSOCIATES, P.C.
Ben Barnow
One N. LaSalle Street, Ste. 4600
Chicago, IL 60602
(312) 621-2000 (p)
(312) 641-5504 (f)
b.barnow@barnowlaw.com

MCSWEENEY/LANGEVIN, LLC
Rhett A McSweeney
David M. Langevin
2116 2nd Avenue South
Minneapolis, Minnesota 55404
(612) 746-4646 (p)
(612) 454-2678 (f)
ram@westrikeback.com

LAW OFFICE OF ARON D. ROBINSON
Aron D. Robinson
180 West Washington St., Suite 700
Chicago, IL 60602
(312) 857-9050 (p)
Adroblaw@aol.com

LOCKRIDGE GRINDAL NAUEN PLLP
Karen H. Riebel
100 Washington Avenue South,
Suite 2200
Minneapolis, MN 55401
(612) 339-6900 (p)
(612) 339-0981 (f)
khriebel@locklaw.com

THE DRISCOLL FIRM, P.C.
John J. Driscoll
Christopher J. Quinn
211 N. Broadway, 40th Floor
St. Louis, MO 63102
(314) 932-3232 (p)
john@thedriscollfirm.com
chris@thedriscollfirm.com

THE COFFMAN LAW FIRM
Richard L. Coffman
505 Orleans St., Suite 505
Beaumont, TX 77701
(409) 833-7700 (p)
(866) 835-8250 (f)
rcoffman@coffmanlawfirm.com

STEWARD LAW FIRM, LLC
John S. Steward
1717 Park Avenue
St. Louis, Missouri 63104
(314) 571-7134 (p)
(314) 594-5950 (f)
Glaw123@aol.com

Attorneys for Appellants

Certificate of Brief Length

The undersigned counsel for Appellants Melissa Alleruzzo, Heidi Bell, Rifet Bosnjak, John Gross, Kenneth Hanf, David Holmes, Steve McPeak, Gary Mertz, Katherin Murray, Christopher Nelson, Carol Puckett, Alyssa Rocke, Timothy Roldan, Ivanka Soldan, Melissa Thompkins, and Darla Young, certifies that this brief complies with the requirements of Fed. R. App. P. 32(a)(7)(B) in that it is printed in 14 point, proportionately spaced typeface utilizing Microsoft Word 2010 and contains 7,942 words, including headings, footnotes, and quotations.

July 12, 2016

LOCKRIDGE GRINDAL NAUEN PLLP

By: /s/ Karen H. Riebel

Karen H. Riebel
100 Washington Avenue South,
Suite 2200
Minneapolis, MN 55401
(612) 339-6900 (p)
(612) 339-0981 (f)
khriebel@locklaw.com

Attorney for Appellant

Certificate of Virus Free

Pursuant to Rule 28A(h)(2) of the Eight Circuit Rules of Appellate Procedure, the undersigned counsel for Appellants Melissa Alleruzzo, Heidi Bell, Rifet Bosnjak, John Gross, Kenneth Hanf, David Holmes, Steve McPeak, Gary Mertz, Katherin Murray, Christopher Nelson, Carol Puckett, Alyssa Rocke, Timothy Roldan, Ivanka Soldan, Melissa Thompkins, and Darla Young, certifies that this brief and the accompanying addendum have been scanned for computer viruses and are virus free.

July 12, 2016

LOCKRIDGE GRINDAL NAUEN PLLP

By: /s/ Karen H. Riebel

Karen H. Riebel
100 Washington Avenue South,
Suite 2200
Minneapolis, MN 55401
(612) 339-6900 (p)
(612) 339-0981 (f)
khriebel@locklaw.com

Attorney for Appellant

Certificate of Service

I hereby certify that on July 12, 2016, I electronically filed the foregoing with the Clerk of the Court of the United States Court of Appeals for the Eighth Circuit by using the CM/ECF system.

July 12, 2016 **LOCKRIDGE GRINDAL NAUEN PLLP**

By: /s/ Karen H. Riebel

Karen H. Riebel
100 Washington Avenue South,
Suite 2200
Minneapolis, MN 55401
(612) 339-6900 (p)
(612) 339-0981 (f)
khriebel@locklaw.com

Attorney for Appellant