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.)

RESPONSE AND REPLY 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

507622.6

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 P.L.L.P.
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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

STATEMENT OF THE CASE

A. Statement of Facts and Relevant Procedural History

Plaintiffs incorporate the Statement of Facts from their Principal Brief. *See* Pls.' App. Br. 4–7. Plaintiffs also incorporate the Relevant Procedural History from their Principal Brief. *See* Pls.' App. Br. 7–8.

B. 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' Consolidated Amended Complaint ("CAC") for lack of subject matter jurisdiction. ADD-1; JA-131. Defendants, through a cross-appeal, seek review as well, arguing that, should this Court hold that Plaintiffs adequately pleaded Article III standing, their claims should nevertheless be dismissed for failure to state a claim upon which relief may be granted. Def. App. Br. 41–42.

SUMMARY OF ARGUMENT

Plaintiffs have standing to bring this suit. Since 2013, the Supreme Court, in several opinions, has repeatedly confirmed that the risk of real harm is sufficient to confer Article III standing. Since 2007, the Ninth, Eleventh, Seventh, and Sixth Circuits have faithfully applied the Supreme Court's instruction and found standing in data breach cases, like this one, where malicious hackers stole the Personal Identifying Information ("PII") of the plaintiffs and class members. Despite the overwhelming weight of authority conferring standing on Plaintiffs in

this matter, Defendants urge this Court to affirm based largely on an appeal to a lone case from the Third Circuit that is distinguishable because the plaintiffs in that matter, unlike Plaintiffs here, failed to allege that their personal information was stolen. Nonetheless, Defendants attempt to analogize this case to the Third Circuit case by twisting and ignoring crucial allegations in the CAC. Defendants similarly disregard the plain allegations of actual economic injury suffered by Plaintiff Holmes, and in doing so, additionally apply an incorrect standard in assessing the Article III traceability of his injury. Finally, Defendants ignore relevant Eighth Circuit precedent in arguing that Plaintiffs do not have standing for their breach of contract claims.

Though not reached by the court below, this Court should not dismiss Plaintiffs claims on other grounds because Plaintiffs adequately pleaded their state and common law claims. Defendants' urge this Court to dismiss Plaintiffs' claims due to a lack of actual injury, but the CAC plainly alleges that Plaintiffs have suffered fraud charges, incurred mitigation costs, and likely will incur the same in the future as a result of Defendants' conduct. These alleged injuries are damages sufficient to support Plaintiffs' claims under the various laws and statutes alleged in the CAC. Defendants further assert various arguments with respect to the viability of each claim pleaded in the CAC. These arguments are either incorrect

or meritless, and have been rejected time and again by state and federal courts throughout the country.

For all of these reasons, the Court should reject Defendants' arguments, reverse the district court, and remand this case for further proceedings.

ARGUMENT

I. PLAINTIFFS HAVE ARTICLE III STANDING TO BRING SUIT

Article III standing consists of three elements: the plaintiff must have (1) suffered injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). "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.'" *Id.* (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). The CAC pleaded all three elements.

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

1. Plaintiffs' More-Than-Plausible Allegations of Actual, Malicious Theft of Personal Information Stored by Defendants Establish Injury-in-Fact

Defendants misstate the first issue presented by this appeal as whether Plaintiffs' standing can be based on "a ***possibility*** that third-party hackers ***might*** have stolen their payment card data from Defendants." Def. App. Br. 2 (emphasis

added). Throughout their Brief, Defendants contend that Plaintiffs fail to allege actual theft of their PII, and argue that criminal hackers merely accessed—but did not steal—Plaintiffs' payment card information. *See* Def. App. Br. 17–20; *see also id.* 6–7, 11. If Defendants' assertion that there was no actual theft should be taken as a facial challenge to the adequacy of Plaintiffs' allegations, that assertion flies in the face of the CAC. Plaintiffs sufficiently allege that their PII was actually stolen during an extensive and sophisticated Data Breach in 2014. If Defendants wish to factually challenge the theft of Plaintiffs' data, they are free to do so at a later stage of litigation. However, Defendants' Rule 12(b)(1) motion to dismiss for failure to allege facts establishing Article III standing is based on a facial challenge, and this Court should not permit Defendants to prevail on arguments that ignore the applicable standard of review. The district court's decision should not stand for the same reason.

In the CAC, Plaintiffs unequivocally allege that hackers stole Plaintiffs' PII, putting their private, financial information at "serious, immediate, and ongoing risk." CAC ¶ 8. In fact, Plaintiffs go above and beyond their pleading obligations by alleging with particularity how the hackers infiltrated Defendants' networks and point-of-sale terminals. CAC ¶¶ 38–44 (alleging how sophisticated hackers breached Defendants' unprotected point-of-sale network, and installed malicious software (RAM scrapper malware) designed to harvest consumer information).

Throughout the CAC, Plaintiffs refer to the release, disclosure, and ***theft*** of their PII. *See, e.g.*, CAC ¶ 61 ("In allowing and making possible the theft of Consumer Plaintiffs' and the other Class members' PII, Defendants failed to meet the standards of commercially reasonable steps that should be taken to protect Consumer Plaintiffs and the Class."); *see also* CAC ¶¶ 60, 70, 78. To suggest that an allegation of data theft is absent from Plaintiffs' Complaint is erroneous.[1]

And certainly, the detailed, factual allegations in Plaintiffs' Complaint are not "threadbare recitals of the elements of a cause of action" denounced by the Supreme Court in *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Rather, Plaintiffs have "asserted facts that affirmatively and plausibly suggest" that their PII was stolen and that they face an impending, substantial risk of identity theft and fraud. *See Zanders v. Swanson*, 573 F.3d 591, 594 (8th Cir. 2009). Moreover, as the Seventh Circuit reasoned in *Remijas v. Neiman Marcus Group, LLC*:

> At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the . . . data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.

794 F.3d 688, 693 (7th Cir. 2015).

[1] As explained in Plaintiffs' opening brief, it is untenable to ignore Plaintiffs' allegations of actual theft, and to instead infer that the hackers engaged in a sophisticated, covert hacking operation over an extended period of time simply for the purpose of accessing (but not stealing) Plaintiffs' PII. *See* Pls.' App. Br. 20.

Defendants' argument that Plaintiffs' reference to a single sentence from a press release in their CAC—for purposes of establishing that the Data Breach might be more expansive than currently believed or admitted—somehow invalidates the remainder of their allegations concerning the theft of Plaintiffs' PII is off base. *See* Def. App. Br. 19–20. And the district court's reliance on that press release *instead of* the Plaintiffs' well-pleaded allegations is similarly flawed. Unlike in *Moses.com Securities, Inc. v. Comprehensive Software Systems, Inc.*, 406 F.3d 1052 (8th Cir. 2005), the press release, while relevant for the factual allegation it supported, is not specifically mentioned by Plaintiffs as a grounds for its claims against Defendants. *See id.* at 1063 n.3.

Even assuming *arguendo* that the press release is incorporated in its entirety into Plaintiffs' CAC, the result is not what the district court concluded, or what Defendants suggest. As stated by this Court in *Deerbrook Pavilion, LLC v. Shalala*, 235 F.3d 1100 (8th Cir. 2000), on a motion to dismiss, a court must primarily consider the allegations in the complaint over any materials referenced in the complaint. *Id.* at 1102 (citing *Jackson v. City of Columbus*, 194 F.3d 737, 745 (6th Cir. 1999); *Sebastian v. United States*, 185 F.3d 1368, 1374 (Fed. Cir. 1999)).

2. Injury-In-Fact Is Established By Allegations of Substantial Risk of Harm Resulting From the Disclosure of Information

Defendants challenge and mischaracterize the standards set forth by the Supreme Court to establish standing. Specifically, Defendants contend that "no harm has materialized" from the "Intrusions". Def. App. Br. 11. Defendants also infer that the only concrete injury that might suffice to confer Article III standing in this matter is an out-of-pocket loss in connection with a fraudulent charge. *See* Def. App. Br. 6 ("No Plaintiff alleges actual injury arising from the misuse of his or her payment card data as a result of the Intrusions."). These statements reflect a fundamental misunderstanding of what constitutes an injury-in-fact under relevant precedent.

First, the "substantial risk" language in *Driehaus* that Defendants challenge, Def. App. Br. 15 n.5, comes directly from *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), where the Supreme Court noted that it had "found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm. *Id.* at 1150 n.5 (citations omitted). Furthermore, the Court made clear in *Spokeo, Inc. v. Robins* that "[t]his does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness." 136 S. Ct. 1540, 1549 (2016). Accordingly, Defendants' misreading of relevant Supreme Court precedent should be disregarded.

Defendants suggest a different, stricter standard for standing applies where private entities are sued. This is incorrect. *Medimmune, Inc. v. Genentech, Inc.*, counsels otherwise. 549 U.S. 118, 134 n.12 (2007) ("Article III does not favor litigants challenging threatened government enforcement action over litigants challenging threatened private enforcement action. Indeed, the latter is perhaps the easier category of cases, for it presents none of the difficult issues of federalism and comity . . . .").

Second, this Court recently intimated that the unauthorized access of sensitive information confers standing. In *Braitberg v. Charter Communications, Inc.*, No. 14-1737, --- F.3d ---, 2016 WL 4698283 (8th Cir. Sept. 8, 2016), the Court found no standing for a Cable Communications Policy Act plaintiff because the plaintiff failed to allege that his personal information had been disclosed or improperly accessed. The Court noted the plaintiff failed to identify any material risk of harm from the mere retention of his data, and further stated that without allegations that his data was disclosed, *or that any outside party had accessed the data*, any risk of harm was speculative or hypothetical. *Id.* at *4. *Braitberg* thus shows that disclosure of information, or improper access by a third-party qualifies as injury-in-fact and is sufficient for purposes of Article III standing.

3. Plaintiffs' Allegations of Theft and the Resultant Substantial and Imminent Risk of Harm Constitute Injury-In-Fact

This Court should follow the reasoning of the Seventh Circuit Court of Appeals in *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016) and *Remijas*, and the Sixth Circuit in *Galaria v. Nationwide Mut. Ins. Co.*, Nos. 15-cv-3386/3387, --- Fed. Appx. ---, 2016 WL 4728027 (6th Cir. Sept. 12, 2016) (unpublished opinion), and find that Plaintiffs' alleged injuries—in particular, their increased risk of fraudulent future charges and identity theft—are precisely the kinds of injuries that can support a lawsuit under *Spokeo*, *Clapper*, and *Driehaus*. *See* Pls.' App. Br. 16–19. Defendants' repeated mischaracterization of Plaintiffs' allegations is a blatant attempt to align the facts of this case with those of a factually distinct case heard—and wrongly decided—by the Third Circuit Court of Appeals in *Reilly v. Ceridian Corp.*, 664 F.3d 38, 44 (3d Cir. 2011). Though the Third Circuit's reasoning in *Reilly* was certainly flawed, both the district court below and Defendants fail to recognize that the allegations made by Plaintiffs here differ markedly from those in *Reilly*.

For instance, in *Reilly* the plaintiffs merely alleged that a firewall was briefly breached on a single occasion; there was no allegation of an "intentional or malicious" intrusion or any identifiable taking. 664 F.3d at 44. Here, unlike in *Reilly*, Plaintiffs allege much more than a one-time breach of a firewall with

unknown intention or results, and there is no doubt that a "taking" of Plaintiffs' personal, sensitive information occurred based on the well-pleaded allegations in the CAC.

The Sixth Circuit recently distinguished *Reilly* on this exact basis, finding *Reilly* "not on point where, as here, Plaintiffs allege an 'identifiable taking'—the intentional theft of their data." *Galaria*, 2016 WL 4728027, at *4. The Sixth Circuit also found *Reilly* unpersuasive because "[w]e must accept as true Plaintiffs' allegations about the nature of the breach and the data stolen, and construe the complaints in Plaintiffs' favor." *Id.* The Court should follow *Galaria*, as well as *Lewert* and *Remijas*, and reject Defendants' arguments.[2]

4. The Passage of Time Since the Breach and the Particularities of Plaintiffs' Mitigation Costs Are Irrelevant

Defendants also contend that Plaintiffs lack standing because they cannot look into the future and determine when and how future fraudulent charges or identity theft might occur. *See* Def. App. Br. 25–28. This argument is baseless. Plaintiffs' alleged injuries, and the basis for their Article III standing, are not minimized or obviated by the passage of time.

[2] Defendants cite *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 654–57 (S.D. Ohio 2014) in support of their erroneous assertion that courts routinely lack subject matter jurisdiction over data breach cases. That opinion was reversed by the Sixth Circuit on September 12, 2016. *See* Case Nos. 15-3386/3387, 2016 WL 4728027, at *6 (6th Cir.).

Defendants' argument and the district court's reasoning demonstrate a fundamental misunderstanding of *Clapper*, *Driehaus*, and *Spokeo* in the data breach context. There is no specific temporal requirement concerning when the future harm might happen. As the Seventh Circuit reasoned in *Remijas*, Plaintiffs "should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, ..." 794 F.3d at 693; *see also In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014); *Galaria*, 2016 WL 4728027, at *3 ("[A]lthough it might not be 'literally certain' that Plaintiffs' data will be misused, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable.").

Similarly, at the pleading stage, Plaintiffs are not required to allege precisely how much time and money they have spent mitigating harm caused by the Data Breach. *See* Def. App. Br. 31. Contrary to Defendants' assertion, none of the allegations in the CAC indicates that these mitigation costs were *de minimis*. *See* Def. App. Br. 31. Because Plaintiffs have adequately alleged a substantial and imminent risk of harm as a result of the Data Breach, the costs that they have reasonably incurred to mitigate the risk of future harm also constitute an injury-in-fact. *See In re Adobe Sys.*, 66 F. Supp. 3d at 1217.

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

Defendants' contention that the CAC fails to allege Plaintiff Holmes' fraud charge is perplexing. At Paragraph 31, the CAC states, "Shortly [after the Breach], Holmes noticed a fraudulent charge on his credit card statement and immediately cancelled his credit card, which took two weeks to replace. As a result of such compromise, Holmes suffered losses and damages in an amount yet to be completely determined, as such losses and damages are ongoing[.]" Plaintiff Holmes suffered a fraud charge and was damaged as a result.

Moreover, Plaintiff Holmes is not, as Defendants contend, required to prove his claim and causation on the pleadings. "Proximate causation is not a requirement of Article III standing." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377, 1391 n.6 (2014); *Carlsen v. GameStop, Inc.*, No. 15-2453, --- F.3d ---, 2016 WL 4363162, at *3 (8th Cir. Aug. 16, 2016) ("[I]t is crucial not to conflate Article III's requirement of injury in fact with a plaintiff's potential causes of action, for the concepts are not coextensive."). "To that end, the fact that an injury is indirect does not destroy standing as a matter of course." *Galaria*, 2016 WL 4728027, at *4. "Rather, the traceability requirement mainly serves to eliminate those cases in which a third party and not a party before the court causes the injury." *Id.*

Here, Plaintiff Holmes has alleged that Defendants' inadequate data security allowed hackers to steal his personal information and make fraudulent charges on his payment card. Plaintiff Holmes also has alleged close proximity between the breach and his fraudulent charges. This is all that is required at this stage of the litigation. *See Galaria*, 2016 WL 4728027, at *4–*5 (upholding similar allegations).

While Defendants seek to require Plaintiff to plead his injury with particularity, including the amount of injury, the date of injury, and the store he shopped at before the injury, this is not a fraud case governed by Fed. R. Civ. P. 9(b). Plaintiff is not required to allege the who, what, where, and how of his injury, but rather only is required to provide Defendant a short and plain statement of his claim. Fed. R. Civ. P. 8(a). Plaintiff has done that here, and the Court should reject Defendants' overly restrictive interpretation of Article III and Rule 8.

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

Similar to their reading of Plaintiff Holmes' injury allegations, Defendants completely misread Plaintiffs' breach of implied contract allegations. Plaintiffs plainly allege that Defendants offered Plaintiffs the option to purchase products with payment cards, and that implicit in this offer was the promise to take reasonable steps to protect Plaintiffs' PII. CAC ¶¶ 137–38. In fact, had such terms not been implied, Plaintiffs, along with most reasonable consumers, would not

have purchased items using their payment cards. CAC ¶ 139. As Plaintiffs purchased goods with their cards, they fulfilled their part of the contract; and as Defendants failed to protect Plaintiffs' PII, Defendants breached their part of the contract. ¶¶ 140–41. This is all that is required at the pleading stage. *See Carlsen*, 2016 WL 4363162, at *3 ("[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.").

Defendants' contention that Plaintiffs' breach of implied contract claim fails for lack of factual support is baseless. Again, Plaintiffs allege that they purchased goods, and would not have purchased those goods using their payment cards had they known Defendant did not intend to safeguard their PII. In fact, no reasonable consumer would use a payment card and expose their personal information to anyone if they knew that person or entity would disclose that information or fail to protect it. That is common sense. The fact that Plaintiffs were divulging sensitive personal information to Defendants, which information when handled improperly, or disclosed to third parties, can cause serious, long-lasting injury supports their breach of implied contract claim. And, in any event, this argument, along with Defendants' damages argument and the others contained in its standing section regarding breach of implied contract, more properly are addressed as a merits question, not one of standing. *See Carlsen*, 2016 WL 4363162, at *3 ("To assert

standing in a breach-of-contract claim, we do not require facts establishing the legal conclusion of a valid, enforceable contract."). As such, the Court should reject Defendants' arguments.

II. PLAINTIFFS' CLAIMS ARE ADEQUATELY ALLEGED

A. The Court Should Remand for the District Court to Decide Defendants' Motion to Dismiss Under Rule 12(b)(6)

Defendants argue that, even if Plaintiffs adequately allege standing sufficient to satisfy Article III, this Court should nevertheless affirm the district court's dismissal under Rule 12(b)(6), and dismiss Plaintiffs' claims with prejudice because they fail to adequately allege sufficient factual matter to support a right to relief. Def. App. Br. 41. This Court may "affirm the judgment below on any ground supported by the record, whether or not raised or relied on in the district court." *A.H. ex rel. Hubbard v. Midwest Bus Sales, Inc.*, 823 F.3d 448, 453 (8th Cir. 2016) (internal alterations and citation omitted). But Defendants are incorrect that this Court must dismiss Plaintiffs' claims with prejudice. Rather, given the factual claims asserted by Plaintiffs, this Court should remand for the district court to decide the issues in the first instance. *See Carlsen*, 2016 WL 4363162, at *4 n.2.

However, if the Court is inclined to address the Rule 12(b)(6) arguments, the Court should deny Defendants' motion. But, if this Court concludes that Plaintiffs lack sufficient facts in their Complaint, Plaintiffs respectfully request that the

Court dismiss their claims without prejudice and with leave to amend. *Accord Knox v. Kempker*, 297 F. App'x 573 (8th Cir. 2008).

B. Legal Standard on a Rule 12(b)(6) Motion to Dismiss

To survive a motion to dismiss under Rule 12(b)(6), a complaint must contain sufficient factual matter, accepted as true, to state a claim for relief that is plausible on its face. *Hamilton v. Palm*, 621 F.3d 816, 817 (8th Cir. 2010) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)) (internal quotations omitted). Although a complaint need not contain "detailed factual allegations," it must contain facts with enough specificity "to raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Adams v. City of Indianapolis*, 742 F.3d 720, 728 (7th Cir. 2014) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). Determining whether a claim is plausible is a context-specific task that requires the reviewing court to draw on its judicial experience and common sense. *Hamilton*, 621 F.3d at 817. When reviewing a motion to dismiss, courts construe the pleadings in the light most favorable to the nonmoving party and facts alleged in the complaint are taken as true. *Insulate SB, Inc. v. Advanced Finishing Sys., Inc.*, No. 13-2664 ADM/SER, 2014 WL 943224, at *4 (D. Minn. Mar. 11, 2014). Plaintiffs' claims meet this standard.

C. Defendants' Choice of Law Analysis is Premature

Defendants argue that this Court should determine which states' law apply as an "initial inquiry." Def. App. Br. 42–44. But at the initial stages of pleading, the Court need not engage in extensive choice-of-law analysis. *See, e.g.*, *Kinetic Co. v. Medtronic, Inc.*, 672 F. Supp. 2d 933, 946 (D. Minn. 2009) (finding that because "class certification is not before the Court . . . [i]t is, therefore, premature to consider choice of law issues or the claims of potential class members in other states."); *In re ConAgra Peanut Butter Prod. Liab. Litig.*, No. 1:07MD1845-TWT, 2008 WL 2132233, *1 (N.D. Ga. May 21, 2008) (agreeing with plaintiffs that "it is premature to conduct a rigorous choice of law analysis at this stage" because "[s]uch an analysis is more appropriate at the class certification stage"); *In re K-Dur Antitrust Litig.*, 338 F. Supp. 2d 517, 541 (D.N.J. 2004) (choice-of-law analysis "premature" at pleading stage). Defendants ask this Court to make factual determinations about where the Data Breach took place; however, the precise location of the Data Breach is a matter for discovery. Defendants rely on factual claims about where "Plaintiffs reside and swiped their cards in Defendants' store locations" that are more properly decided after discovery and at the class certification stage. Regardless, even applying Defendants' choice of law analysis to follow the laws of the states where named plaintiffs reside, Plaintiffs' claims have been adequately pleaded.

D. Plaintiffs' Negligence and Negligence *Per Se* Claims Are Well-Pleaded

In their brief, Defendants argue that Counts III and V should be dismissed because (a) Plaintiffs fail to plead cognizable injuries; (b) the economic loss doctrine bars Plaintiffs' negligence claims; and, (c) Plaintiffs fail to allege that Defendants breached a duty. Def. App. Br. 44–48.

In order to adequately plead negligence, Plaintiffs need to allege four elements: duty, breach, causation, and injury. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1170 (D. Minn. 2014) (citing *Schmanski v. Church of St. Casimir of Wells*, 67 N.W.2d 644, 646 (1954)). These elements are substantially the same in all the jurisdictions where Plaintiffs reside, and this Court need not do a separate analysis by state. *See Cramer v. Slater*, 204 P.3d 508, 513 (Idaho 2009); *Polzo v. Cnty. of Essex*, 960 A.2d 375, 384 (N.J. 2008); *Patton v. U.S. Rugby Football Union, Ltd.*, 851 A.2d 566, 570 (Md. 2004); *Reilly v. Tiergarten Inc.*, 633 A.2d 208, 210 (Pa. 1993); *Martin v. Washington*, 848 S.W.2d 487, 493 (Mo. 1993); *Wojdyla v. Park Ridge*, 592 N.E. 2d 1098, 1100 (Ill. 1992). Plaintiffs adequately pleaded all four elements of their negligence claim. CAC ¶¶ 119–35.

1. Plaintiffs Allege Cognizable Injuries

First, Defendants argue that Plaintiffs' negligence claim fails to plead cognizable injuries because the injuries are "intangible," rely on "disclosure," or are mitigation damages. Def. App Br. 45–46. Courts across the country have

repeatedly rejected this argument in the data breach context, and the Court should do so here as well.

Three separate district courts have turned away arguments similar to those made by the defendants in the data breach class action context. First, the Southern District of Illinois recently turned away a defendant's similar arguments for dismissing the plaintiffs' negligence and negligence *per se* claims. *Allen v. Schnuck Markets, Inc.*, Civ. No. 15-cv-0061-MJR-DGW, 2015 WL 5076966 (S.D. Ill. Aug. 27, 2015). The defendant challenged whether the complaint properly pleaded injury and damages. *Id.* at *2. The court reasoned that the plaintiffs' complaint:

> makes it over the plausibility threshold. . . . [T]he pleadings contain more than . . . unsupported, conclusory allegations . . . . Each Plaintiff adopts Paragraph 233 of the Complaint, which states in pertinent part that Plaintiffs have suffered and will continue to suffer financial losses caused by fraudulent charges to their compromised cards and bank fees associated with the data breach . . . . In addition to any noneconomic harm, here Plaintiffs clearly[] allege they have already suffered economic harm due to the Schnucks data breach . . . . As it pertains to the instant motion, which targets only the sufficiency of the Complaint vis-à-vis the damages prong of each claim, that is all the Federal Rules require.

Id. at *3.

Second, the district court in *Corona v. Sony Pictures Entertainment, Inc.* rejected the notion that victims of a massive data breach had not alleged a cognizable injury. No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at *3 (C.D.

Cal. June 15, 2015). In that putative class-action case, hackers stole nearly 100 terabytes of sensitive personal data on at least 15,000 Sony employees. *Id.* at *1. Plaintiffs alleged that, as a result of the breach, they had to purchase identity-protection services and insurance and take other measures to protect their compromised information, and that they remained vulnerable to identity theft, medical theft, tax fraud, and financial theft. *Id.* at *1. Ruling on Sony's motion to dismiss, the court found, *inter alia*, that "the Complaint sufficiently alleges facts to support the reasonableness and necessity of Plaintiffs' credit monitoring" and that the data breach had "drastically increase[d] their risk of identity theft." *Id.* at *4. Thus, the court sustained the plaintiffs' negligence claims as to costs relating to credit monitoring, identity-theft protection, and penalties. *Id*.

Third, the Northern District of California recently reached the same result in a case involving the breach of a social-networking site's user credentials. *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855 (N.D. Cal. 2011). In *Claridge*, the plaintiff sued after a hacker downloaded the e-mail and log-in credentials of 32 million RockYou users, including his own. *Id.* at 859. The court denied the defendant's motion to dismiss the plaintiff's negligence and negligence *per se* claims, "conclud[ing] that plaintiff's allegations that he was injured by defendant's actions in permitting the unauthorized and public disclosure of his Private Information,

which had some unidentified but ascertainable value, are sufficient to allege an actual injury at this stage." *Id.* at 866.[3]

At the very least, other Circuit Courts of Appeals have held that mitigation expenses and costs are cognizable injuries under black-letter negligence law. The First Circuit, in evaluating mitigation damages, noted that "courts award mitigation costs even when it is not certain at the time that these costs are needed, when mitigation costs are sought but other damages are unavailable, and when mitigation costs exceed the amount of actual damages." *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 163 (1st Cir. 2011); *see also id.* at 162–63 (collecting cases and citing Restatement (Second) of Torts § 919). Other Circuit Courts, including the Sixth and Seventh Circuits recently, have recognized the "aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit-card numbers are changed, and to pursue relief for unauthorized charges." *Remijas*, 794 F.3d at 692; *see also Galaria*, 2016 WL 4728027, at *3. "There are identifiable costs associated with the process of sorting things out." *Remijas*, 794 F.3d at 692.

[3] *See also, e.g.*, *Target*, 66 F. Supp. 2d 1154, 1171 (D. Minn. 2014) (finding plaintiff's negligence claims to consist of a "short and plain statement," as required by Fed. R. Civ. P. 8(a)(2), "that plausibly alleges that Plaintiffs suffered damage as a result of the delay"); *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327–28 (11th Cir. 2012) ("Plaintiffs meet the pleading standards for their allegations on the counts of negligence, negligence per se," and other causes of action).

Plaintiffs' allegations plausibly pleaded actual and cognizable injuries under these standards. First, all sixteen Plaintiffs and all Class members suffered the theft of their sensitive personal and financial information, decreasing the security of their bank accounts, making their identities less secure, and subjecting them to the significant threat of identity theft. CAC ¶ 133. They have and will have to incur time and money to protect their bank accounts and identities and protect against the heightened risk of identity theft for years to come. *Id.* Even aside from the money, their time has value. *See Remijas*, 794 F.3d at 692–93; *Galaria*, 2016 WL 4728027, at *3.

Defendants recognize the significant risks that Plaintiffs now face as a result of the Data Breach and the fact that Plaintiffs have suffered damages. For example, in a Press Release issued on August 14, 2014, Defendant Supervalu "urge[d] customers to be vigilant and closely review or monitor their bank and credit-card statements, credit reports and other financial information for any evidence of identity theft or other unusual activity." *See Supervalu Notifies Customers of Criminal Computer Intrusion at Some of Its Owned and Franchised Stores* at 3 (Aug. 14, 2014) [ECF No. 36-1].

In addition, the CAC alleges additional harm to two of the sixteen Plaintiffs. Shortly after the Data Breach, David Holmes noticed a fraudulent charge on his credit-card statement and had to take steps to cancel and replace the card, incurring

losses and damages in an amount to be determined. CAC ¶ 31. Kenneth Hanff incurred costs and expenses associated with closing his checking account and opening a new one to prevent fraudulent purchases. CAC ¶ 18. Notably, cancelling and opening new credit cards impacts a person's credit rating.

In the current climate, it is well-known that breaches are aimed at, and often lead to, identity theft. "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas*, 794 F.3d at 693; *see Galaria*, 2016 WL 4728027, at *4; *see also In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) (finding it obvious that "hackers intend to misuse the personal information stolen in the 2013 data breach [and that] they will be able to do so"). The CAC sets forth the common and oftentimes significant consequences of identity theft. Even Defendants' data-breach-notification letters acknowledge the risk the Data Breach created. *See, e.g.*, ECF No. 36-1, 5–8 (ECF pagination) ("Consumer Identity Protection Reference Guide"). Plaintiffs' mitigation costs and expenses were therefore indisputably reasonable, cognizable, and compensable.

Finally, and importantly, Plaintiffs have also alleged that "illicit websites are selling the stolen payment card PII 'dumps' to international card counterfeiters and fraudsters." CAC ¶ 9. This fact allegation deserves to be fleshed out in discovery.

In the meantime, in light of the identity theft and fraud that have occurred after other data breaches, it is sufficiently plausible to advance beyond the pleading stage. *See, e.g.*, *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 120 (2d Cir. 2010) (holding that "[t]he *Twombly* plausibility standard . . . does not prevent a plaintiff from pleading facts alleged 'upon information and belief' where the facts are peculiarly within the possession and control of the defendant . . . or where the belief is based on factual information that makes the inference of culpability plausible") (citations and internal quotation marks omitted).[4]

Defendants attempt to inject into this Court's analysis the inappropriate, unsupported, and self-serving proposition that there is no evidence of any misuse of consumer data, and that Plaintiffs do not allege such. *See* Def. App. Br. 45–46. But this is simply not true. Rather, for purposes of this motion, the Court should accept as true the converse: that, as Plaintiffs pleaded, there is evidence that consumer data has been misused. CAC ¶¶ 8–9, 31, 62–82. Even if they were appropriate in a Rule 12 motion to dismiss, Defendants' assertions in this regard are of no probative value, moreover, because Defendants do not indicate that the investigations they allegedly undertook would have uncovered misuse. This Court

[4] *See also Van Stelton v. Van Stelton*, No. C11-4045-MWB, 2013 WL 3776813, at *10 (N.D. Iowa July 17, 2013) (collecting decisions allowing "information and belief" pleading); *Frerck v. Pearson Educ., Inc.*, No. 11–cv–5319, 2012 WL 1280771, at *3 (N.D. Ill. Apr. 16, 2012) (same).

should follow the persuasive logic of the district courts and other Circuit Courts of Appeals cited and conclude that Plaintiffs adequately pleaded cognizable injuries.

2. The Economic Loss Doctrine Does Not Bar Plaintiffs' Negligence Claims

Defendants also argue that Plaintiffs' negligence claims should be dismissed based on the economic loss doctrine. Def. App. Br. 46–47. For multiple reasons, the doctrine is inapplicable here, and this Court should decline to adopt it in this context.

Every state has some version of the economic loss doctrine, which, generally speaking, is meant to keep contract law and tort law separate. "It reflects the belief 'that tort law affords the proper remedy for loss arising from personal injury or damages to one's property, whereas contract law and the Uniform Commercial Code provide the appropriate remedy for economic loss stemming from diminished commercial expectations without related injury to person or property.'" *Target*, 66 F. Supp. 3d at 1171 (quoting *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011)). To that end, the rule "bars a plaintiff from recovering for purely economic losses under a tort theory of negligence." *Id.* The court-made rule "is an attempt to prevent contract law from 'drown[ing] in a sea of tort.'" *George v. Uponor Corp.*, 988 F. Supp. 2d 1056, 1069 (D. Minn. 2013) (quoting *E. River S.S. Corp. v. Transamerica Delaval, Inc.*, 476 U.S. 858, 866 (1986)).

The economic loss doctrine has exceptions, which are relatively common among the states. First, economic losses are recoverable in tort for the breach of an independent duty not arising from the parties' contract (assuming there is a contract). *See, e.g.*, *Kerr v. Fed. Emergency Mgmt. Agency*, 113 F.3d 884, 887 (8th Cir. 1997) (applying Missouri law and recognizing that economic losses flowing from independent duties are recoverable) (citations omitted); *Bilt-Rite Contractors, Inc. v. Architectural Studio*, 866 A.2d 270, 288 (Pa. 2005) (favorably citing South Carolina standard that "[a] breach of duty arising independently of any contract duties between the parties . . . may support a tort action"); *Saltiel v. GSI Consultants, Inc.*, 788 A.2d 268, 279–80 (N.J. 2002) ("Under New Jersey law, a tort remedy does not arise from a contractual relationship unless the breaching party owes an independent duty imposed by law."); *Congregation of the Passion v. Touche Ross & Co.*, 636 N.E.2d 503, 515 (Ill. 1994) ("The economic loss doctrine does not bar recovery in tort for the breach of a duty that exists independently of a contract."); *Jacques v. First Nat'l Bank*, 515 A.2d 756, 759–60 (Md. 1986) (explaining that when an independent duty exists and there is an "intimate nexus," such as a contract, between the parties, tort liability arises from "the failure to exercise due care," even when only economic loss ensues).

Second, in some states, the economic loss rule will not bar a negligence claim for pecuniary loss if there is a "special relationship" between the parties or

the occurrence of a "unique circumstance" requires a different allocation of risk. *E.g.*, *Kayser v. McClary*, 875 F. Supp. 2d 1167, 1175 n.5 (D. Idaho 2012) (citations omitted), *aff'd*, 544 F. App'x 726 (9th Cir. 2013); *Freedom Props., L.P. v. Lansdale Warehouse Co.*, No. 06-5469, 2007 WL 2254422, at *6 (E.D. Pa. Aug. 2, 2007) ("[T]he economic loss doctrine is not a bar when two parties have a special relationship such that a negligent party can foresee harm to the plaintiff.").[5] In short, the line drawn between contract and tort turns on the relationship of the product at issue and the consequent failure of what the product was supposed to accomplish. *Moorman Mfg. Co. v. Nat'l Tank Co.*, 435 N.E.2d 443, 455–56 (Ill. 1982) (Simon, J., specially concurring). Hazards peripheral to a product's function, which could not have been anticipated in the commercial "bargain," are properly left to the tort system. *See id.* "[A] defect that endangers personal safety presents an unusually strong attraction to the tort system." *Id.* at 456.

Here, the economic loss rule does not bar Plaintiffs' claims because both exceptions noted above apply and the principles behind the economic loss rule do not support its application. Even if Plaintiffs had an implied contract with Defendants as alleged in the CAC, *see* ¶¶ 136–42, the CAC alleges that Defendants

[5] To the extent Minnesota law applies, the economic loss rule would not bar Plaintiffs' negligence claims because Minnesota's version of the rule applies only to "product defect tort claim[s]." *See* Minn. Stat. § 604.101, subd. 3; *Ptacek v. Earthsoils, Inc.*, 844 N.W.2d 535, 538–39 (Minn. Ct. App. 2014) (explaining that economic loss rule applies only to claims involving product defects and misrepresentation).

had an *independent* duty to safeguard consumers' data and warn them of any breach of their system, arising from Defendants' solicitation of Private Information and representation of reasonable measures that would safeguard it, as well as the sensitivity of the data and the foreseeability of the harm if the data were compromised. CAC ¶¶ 121–31, 134; *see also Congregation of the Passion*, 636 N.E.2d at 515 (finding accounting firm breached independent duty of professional competence).[6]

Plaintiffs also allege that a special relationship exists between them and the Class and Defendants, arising from Defendants' solicitation of Private Information and representation of reasonable measures that would safeguard it. CAC ¶ 120. That is, "Plaintiffs' allegations . . . are that they reposed trust in [Defendants] or that [Defendants] bore a fiduciary-like responsibility to safeguard their financial

[6] The court in *Target* found that the Illinois economic loss rule doomed the Illinois plaintiffs' negligence claim. *See Target*, 66 F. Supp. 2d at 1174 (citing *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528–530 (N.D. Ill. 2011)). Plaintiffs here respectfully disagree and suggest that *In re Michaels* misreads *Moorman Mfg. Co. v. Nat'l Tank Co.*, 435 N.E.2d 443 (Ill. 1982). The *In re Michaels* analysis notwithstanding, *Moorman* did not state that the economic loss rule had only "three exceptions." *See* 435 N.E.2d at 448–52. More to the point, *Moorman* explained that while "qualitative defects" to a product are best handled by contract law, "[t]ort theory is appropriately suited for personal injury or property damage resulting from a sudden or dangerous occurrence" involving a product. 435 N.E.2d at 450. The data breach here is more analogous to a sudden or dangerous occurrence involving a product—the product being the processing of plaintiffs' payment information, the release of which stands to unleash identity theft and other harms on plaintiffs—than a mere qualitative defect in a product resulting in commercial disappointment. *See* CAC ¶¶ 3–13, 38–42, 60, 125–26 (explaining data-breach events).

information. Plaintiffs have plausibly pleaded the existence of a special relationship that . . . courts would recognize as an exception to the economic loss rule." *Target*, 66 F. Supp. 3d at 1175–76. Plaintiffs' allegations support the reallocation of risk from consumers to Defendants, who were the only ones who could implement systems to protect the data. CAC ¶¶ 120–35. Defendants simply do not refute these claims in their briefing.[7]

Because these exceptions to the economic loss doctrine are sufficiently pleaded, Plaintiffs' negligence claims should go forward.

3. Defendants Owed a Duty to Plaintiffs to Protect Their Private Information from Foreseeable Criminal Cyberattacks

Negligence law generally imposes a duty of reasonable care when a defendant's conduct creates a foreseeable risk of injury to a foreseeable plaintiff. *Target*, 64 F. Supp. 3d at 1308 (quoting *Domagala v. Rolland*, 805 N.W.2d 14, 23 (Minn. 2011)); *see also Simpkins v. CSX Transp., Inc.*, 965 N.E.2d 1092, 1096–97 (Ill. 2012); *Phillips v. Cricket Lighters*, 841 A.2d 1000, 1008–09 (Pa. 2003); *Acuna v. Turkish*, 930 A.2d 416, 424 (N.J. 2007); *Patton*, 851 A.2d at 571; *Lac v. Ward Parkway Shopping Ctr. Co.*, 75 SW 3d 247, 267 (Mo. 2002); *Coghlan v. Beta*

[7] Defendants substantially condense their arguments from those made at the motion to dismiss stage in front of the district court. This Court should not expand the arguments made by Defendants – only those arguments raised on appeal are relevant. *See Griffith v. City of Des Moines*, 387 F.3d 733, 739 (8th Cir. 2004) (deeming arguments made at the district court but not briefed on appeal abandoned).

Theta Pi Fraternity, 987 P.2d 300, 311 (Idaho 1999). Inaction on the part of a defendant constitutes negligence when done in disregard of a duty to act for the protection of others. *Domagala*, 805 N.W.2d at 22–23.

Defendants incorrectly argue that there is no duty to protect Plaintiffs from the "intentional criminal conduct of unknown third persons." Def. App. Br. 47–48 (quoting *Meadows v. Friedman R.R. Salvage Warehouse*, 655 S.W.2d 718, 721 (Mo. Ct. App. 1983). The element of duty is ultimately a question of policy. *Erickson v. Curtis Inv. Co.*, 447 N.W.2d 165, 169 (Minn. 1989). Defendants have a duty to exercise reasonable care and caution; it is their conduct that facilitated the foreseeable, inevitable, criminal conduct.

Courts have repeatedly found a duty in data-breach cases. *See*, *e.g.*, *Sony*, 996 F. Supp. 2d at 966 ("[B]ecause Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach."); *Target*, 64 F. Supp. 3d at 1310 ("Plaintiffs have adequately pled that Target owed them a duty of care, and their negligence claim will not be dismissed on this basis"); *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327–28 (11th Cir. 2012) ("Plaintiffs meet the pleading standards for their allegations on the counts of

negligence [and] negligence per se . . . ."); *In re Zappos.com, Inc.*, 3:12-cv-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013) ("Zappos owed Plaintiffs . . . the duty to act as a reasonable and prudent person under the same or similar circumstances."); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F. Supp. 2d 183, 193–95 (M.D. Pa. 2005) (finding plaintiffs met Pennsylvania's five-element duty standard), *aff'd*, 533 F.3d 162 (3d Cir. 2008); *cf. Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, 394 F. Supp. 2d 283, 287 (D. Me. 2005) (finding that defendants' motion to dismiss arguments regarding to duty and the economic loss doctrine to "hinge upon issues of fact as to the nature of the relationships between the parties that the Court may not appropriately resolve via a motion to dismiss").

Defendants owed Plaintiffs a duty to exercise reasonable care in handling and using their PII and protecting it from being stolen, accessed, and misused by unauthorized parties. CAC ¶ 121. Defendants also owed a duty to timely and accurately disclose the scope, nature, and occurrence of the Data Breach. CAC ¶ 124. This duty was owed for several reasons, including that Plaintiffs and the other Class members constituted a well-defined, foreseeable, and probable group of individuals who could foreseeably be injured by inadequate data security, Defendants knew that data security was of prime importance, that the mass quantities of data they handled was of interest to hackers, that their security practices were inadequate and unreasonable, and that hackers routinely attempt to

exploit such vulnerable systems. CAC ¶¶ 122–23. Plaintiffs explain in detail why the breach was entirely avoidable and foreseeable by Defendants. CAC ¶¶ 46–61.

Thus, the CAC plausibly alleges that Defendants owe a duty to Plaintiffs. Recognizing Defendants' duty here fulfills the policy inherent in negligence law—that of compensation for victims and deterrence to future offenders—by placing the risk of financial loss on the only entity with the ability to prevent the loss. To impose a duty here is necessary to spur Defendants and other businesses to implement and maintain reasonable, industry-standard data-security measures. Otherwise, large data handlers will remain careless with consumers' private, sensitive personal information and massive data breaches and their consequences will continue.

Defendants also owed Plaintiffs a duty because of the special relationship between the parties, and Defendants incorrectly assert that Plaintiffs did not plead such. *See* Def. App. Br. 48; *cf.* CAC ¶ 120 (alleging Defendants owed a duty by virtue of their special relationship with Plaintiffs and the other Class members, arising from the understanding that Defendants would not only guard customers' sensitive personal data, but were also in a superior position to do so).

A defendant owes a duty to protect a plaintiff when action by a third party creates a foreseeable risk of harm to the plaintiff and the defendant and plaintiff stand in a special relationship. *See Target*, 64 F. Supp. 3d at 1308 (citing

Domagala, 805 N.W.2d at 23). This duty counters the general proposition that a defendant generally does not have a duty to warn or protect others from harm caused by third party conduct. *Domagala*, 805 N.W.2d at 23; *see also Simmons v. Homatas*, 925 N.E. 2d 1089, 1099 (Ill. 2010); *Baccus v. Ameripride Servs., Inc.*, 179 P.3d 309, 313 (Idaho 2008); *Champion ex rel. Ezzo v. Dunfee*, 939 A.2d 825, 831 (N.J. Super. Ct. App. Div. 2008); *Pendleton v. State*, 921 A.2d 196, 210–14 (Md. Ct. App. 2007); *T.A. v. Allen*, 669 A.2d 360, 362–63 (Pa. Super. Ct. 1995); *Advance Rental Ctrs., Inc. v. Brown*, 729 S.W.2d 644, 645–46 (Mo. Ct. App. 1987); Restatement (Second) of Torts § 315; *cf. Donaldson v. YWCA*, 539 N.W.2d 789, 792 (Minn. 1995) (noting that a special relationship may exist when "the plaintiff is in some respect particularly vulnerable and dependent on the defendant, who in turn holds considerable power over the plaintiff's welfare").

A data breach setting such as the one alleged here can create such a special relationship between the parties. *See Corona*, 2015 WL 3916744, at *5 (finding plaintiffs' allegations, taken as true, sufficiently established a special relationship between employer and employees); *Bell v. Mich. Council 25 of Am. Fed'n of State, Cnty., and Mun. Emps.*, No. 246684, 2005 WL 356306 (Mich. Ct. App. Feb. 15, 2005) (holding that a special relationship can exist such that a defendant owes plaintiffs a duty to protect them from identity theft by safeguarding "the security of their most essential confidential identifying information, information which easily

could be used to appropriate a person's identity"), *permission to appeal denied*, 707 N.W.2d 597 (2005).

The existence of a special relationship is a fact question that cannot be resolved on a motion to dismiss. *See Velez v. City of New York*, 730 F.3d 128, 135 (2nd Cir. 2013) (citing *Applewhite v. Accuhealth, Inc.*, 995 N.E.2d 131, 143–44 (N.Y. 2013)); *Tidikis v. Network for Med. Commc'ns & Research, LLC*, 619 S.E.2d 481, 484–85 (Ga. Ct. App. 2005); *Scottsdale Ins. Co. v. Transp. Leasing/Contract, Inc.*, 671 N.W.2d 186, 195 (Minn. Ct. App. 2003) (noting that where facts are disputed, finder of fact must resolve dispute before court can determine whether special relationship and thus duty exists).

For these reasons, the Court should reject Defendants' arguments and recognize their duty to Plaintiffs and the Class. At the very least, fact questions about the foreseeability of the Data Breach, the likely harm to consumers, and the relationship between the parties preclude resolving the duty issue at the pleading stage. *Banknorth*, 394 F. Supp. 2d at 287.

E. Plaintiffs Allege Claims For Negligence *Per Se*

Defendants challenge Plaintiffs' ability to bring a negligence *per se* claim under section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), which renders unlawful a merchant's failure to reasonably protect consumers'

sensitive information, or state law. Def. App. Br. 48–49. As explained below, Plaintiffs have properly stated a claim for negligence *per se*.[8]

1. Negligence *Per Se* Claims can be Premised on Section 5 of the FTCA

Negligence *per se* "is a form of ordinary negligence that results from violation of a statute." *Anderson v. State*, 693 N.W.2d 181, 189 (Minn. 2005) (citation omitted). In a negligence *per se* claim, a plaintiff seeks to hold defendant liable "because the defendant violated a statute." *Id.* at 190. Such a claim "substitutes a statutory standard of care for the ordinary prudent person standard of care, such that a violation of a statute (or an ordinance or regulation adopted under statutory authority) is conclusive evidence of duty and breach." *Id.* at 189–90 (citation omitted).

Plaintiffs have adequately alleged negligence *per se* here based on the violation of Section 5 of the FTCA. Negligence *per se* liability can be, and has been, premised on the violation by the FTCA in courts throughout the country. *See Bans Pasta, LLC v. Mirko Franchising, LLC*, No. 7:13-cv-00360-JCT, 2014 WL 637762, at *12–14 (W.D. Va. Feb. 12, 2014); *Legacy Acad., Inc. v. Mamilove, LLC*, 761 S.E.2d 880, 892–93 (Ga. Ct. App. 2014), *rev'd in part on other grounds*, 771 S.E.2d 868 (Ga. 2015). This is not "bootstrap[ping] a private cause of

[8] As Defendants note, Plaintiffs concede that Defendants' violation of section 5 of the FTCA does not give rise to negligence *per se* claims under Illinois and Maryland law.

action;" rather, it is exactly the sort of claim for which negligence *per se* is intended.

This case is analogous to the one decided in *Bans Pasta*, and this Court should endorse its reasoning. In *Bans Pasta*, the defendants made the same argument as Defendants here—that the plaintiff's negligence *per se* claim should be dismissed because the FTCA did not give rise to a private cause of action. 2014 WL 637762, at *12. Allowing the claim to go forward, the defendants contended, would allow the plaintiff to evade that lack of a private cause of action. *Id.* The court allowed the claim to go forward. *Id.* at *12–14. The claim survived because, among other factors, the plaintiffs had pleaded the requirements for a negligence *per se* claim: that the defendants violated the statute or rule in question; the rule dictated a standard of conduct or care; the plaintiffs fell within the class of persons the statute was intended to protect;[9] the harm complained of was the same harm the statute was intended to guard against;[10] and violation of the statute proximately caused the plaintiff's injury. *Id.*

Here, as in *Bans Pasta*, Plaintiffs pleaded the required elements: Defendants violated the statute or rule in question (CAC ¶ 145); the rule dictated a standard of

[9] *See Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *1 (3d Cir. Aug. 24, 2015) (affirming district court holding that Federal Trade Commission has authority to bring administrative actions against companies that fail to protect consumer data against hackers).

[10] *See Wyndham*, 2015 WL 4998121, at *1.

conduct or care (CAC ¶ 144); Plaintiffs fell within the class of persons the statute was intended to protect (CAC ¶ 146); the harm complained of was the same harm the statute was intended to guard against (CAC ¶ 147); and Defendants' violation of the statute proximately caused Plaintiffs' injury (CAC ¶ 148). Plaintiffs' claim should be allowed to proceed.

2. Plaintiffs' Claims Fit Within the Standard Negligence *Per Se* Framework

Defendants argue that Plaintiffs may not plead their negligence *per se* claims because they do not allege a physical injury in the way of negligence *per se* cases. Though negligence *per se* claims often arise in cases involving physical injury, they are *not* strictly limited to those circumstances. *See Johnson v. Paynesville Farmers Union Co-Op.*, 817 N.W.2d 693, 706–12 (Minn. 2012) (discussing whether federal organic-produce regulation supported negligence *per se* claim, without indication that negligence *per se* claim was inappropriate for lack of physical injury); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 866 (N.D. Cal. 2011) (declining to dismiss negligence *per se* claim premised on defendant's alleged violation of the federal Stored Communications Act); *Hoskins v. Jackson Grain Co.*, 63 So.2d 514, 515 (Fla. 1953) (violation of a statute regulating the labeling of seed offered for sale constituted negligence *per se*). Defendants' argument that a violation of a "safety statute" is required is simply incorrect. Def.

App. Br. 49 (citation omitted). This Court should decline to impose such a standard.

Additionally, even if a negligence *per se* claim in the relevant states requires injuries to a person or property, Plaintiffs *have* adequately pleaded that they were injured by the Data Breach, and allege damage to both persons and property. *See* CAC ¶¶ 8–9, 16–32, 82, 102, 109, 115, 132–33; *supra* Part II.D.1.

Finally, counter to Defendants' claims, negligence *per se* claims are viable in New Jersey. *See Alloway v. Bradlees, Inc.*, 723 A.2d 960, 967 (N.J. 1999) (holding that federal occupational-safety regulations were "pertinent in determining the nature and extent of any duty of care"); *Eaton v. Eaton*, 575 A.2d 858, 866 (N.J. 1990) (holding violation of careless-driving statute was negligence *per se* because statute specifically incorporated common-law standard of care); *Meder v. Resorts Int'l Hotel*, 573 A.2d 922, 926 (N.J. App. Div. 1989) ("violation of the obligations imposed by . . . federal regulations supports a tort claim under state law"), *cert. denied*, 583 A.2d 310 (N.J. 1990). Thus, a violation of Section 5 can support a negligence *per se* claim in New Jersey.

F. Plaintiffs State a Claim for Breach of Contract Implied in Fact

A contract implied in fact is one inferred from the circumstances and conduct of the parties. *Cooper v. Lakewood Eng'g and Mfg. Co.*, 874 F. Supp. 947, 955 (D. Minn. 1994). An implied contract is in all respects a true contract requiring

a meeting of the minds and differs from an express contract mainly in the manner mutual assent is proved. *Upsher-Smith Labs., Inc. v. Mylan Labs., Inc.*, 944 F. Supp. 1411, 1433 (D. Minn. 1996). Whether a contract is to be implied in fact and its constituent terms are usually determined by the trier of fact. *Bergstedt, Wahlberg, Berquist Assocs., Inc. v. Rothchild*, 225 N.W.2d 261, 263 (Minn. 1975).

Numerous courts have upheld implied contract claims under circumstances similar to those alleged here. In *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011), for example, the First Circuit affirmed the district court's denial of defendant's motion to dismiss consumers' breach of implied contract claim in a data breach case, finding that "a jury could reasonably find an implied contract between [the grocery chain] and its customers that [the chain] would not use the credit-card data for other people's purchases, would not sell the data to others, and would take reasonable measures to protect the information." 659 F.3d at 159. The Court reasoned:

> When a customer uses a credit card in a commercial transaction, she intends to provide that data to the merchant only. Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract.

Id. Similarly, in *Michaels,* the court denied the data-breach retailer's motion to dismiss consumers' implied contract claim because "the allegations demonstrate the existence of an implicit contractual relationship between Plaintiffs and [the

retailer], which obligated [the retailer] to take reasonable measures to protect Plaintiffs' financial information and notify Plaintiffs of a security breach within a reasonable amount of time." 830 F. Supp. 2d at 531. *Target* reached the same conclusion, finding that "Plaintiffs have plausibly alleged the existence of an implied contract" on these facts and that "a determination of the terms of the alleged implied contract is a factual question that a jury must determine." 66 F. Supp. 3d 1176–77. For the same reasons, Defendants' arguments do not avail.

Here, Defendants are Level 1 merchants who accept certain types of credit and debit cards as payment at their stores. CAC ¶ 55. Implicit in the offer to accept credit and debit cards is a contractual obligation on Defendants to implement reasonable security on their network to protect Plaintiffs' and the other Class members' financial information. CAC ¶ 138. The meeting of the minds occurred when Plaintiffs swiped their cards at Defendants' checkout counters. Plaintiffs' payments provide consideration. And, as argued above and throughout, Plaintiffs have alleged cognizable injuries resulting from Defendants' failure to implement adequate security in the form of failure to receive a bargained for benefit, consequential damages for fraudulent charges, and reasonable time and costs in mitigation of the breach. CAC ¶¶ 16–32. Plaintiffs have pleaded facts sufficient to defeat Defendant's motion to dismiss the breach of implied contract claim.

G. Plaintiffs State Claims Under the Consumer-Protection Laws

The CAC plausibly states a claim under the various state consumer-protection laws. Defendants' deficient security and monitoring of their payment-processing network, which facilitated the nearly month-long (and possibly longer) Data Breach, thereby exposing the financial accounts of millions of consumers to the substantial risk of identity theft, is actionable as unfair or deceptive.

The Federal Trade Commission and the various state consumer-protection laws, which draw upon it, prohibit "unfair or deceptive acts or practices." 15 U.S.C. § 45(a); Cal Bus. and Prof. Code § 17200; Idaho Code § 48-603; 815 Ill. Comp. Stat. 505/2; Md. Code, Com. Law § 13-303; Minn. Stat. §§ 325D.44 subd. 1, 325F.69, subd. 1; Mo. Stat. § 407.020; N.J. Stat. § 56:8-2; 73 Pa. Stat. § 201-3. The FTC has enforced section 45 against numerous companies when their deficient cybersecurity facilitated data breaches and exposed consumers' sensitive information. *See Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd* 2015 WL 4998121 (FTC charged that Wyndham violated both deception and unfairness prong in connection with its failure to maintain reasonable and appropriate data security for consumers' sensitive personal information); *see, e.g.*, 76 Fed. Reg. 7213, 7313–14 (Feb. 9, 2011) (FTC filed and settled complaints against several companies based on their failure to "[d]evelop and disseminate comprehensive written information security policies[,]

. . . assess the risks of allowing end users with unverified or inadequate security to access consumer reports through their online portals[,] . . . and [] take appropriate action to correct existing vulnerabilities or threats to personal information in light of known risks").

In *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015), the Third Circuit affirmed an interpretation of § 45(a) that considered deficient cybersecurity over consumer information an unfair practice. *Id.* at *6. There, as here, the defendant was accused of using easily guessed passwords, failing to use readily available security measures (such as firewalls to limit access between network segments), failing to adequately restrict the access of third parties to its network, and failing to employ reasonable measures to detect, prevent, and respond to unauthorized access. *Id.* at *2. The court held that a "company does not act equitably when it . . . fails to make good on [a] promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business." *Id.* at *5. The court noted that, even absent such a promise, the court would consider the conduct unfair and not reasonably avoidable by consumers. *See id*. at *6 n.5.

The CAC at ¶ 100 alleges:

> Defendants' failure to maintain reasonable and adequate computer systems and data security practices, Defendants' fraudulent and

> deceptive omission and/or representations regarding the security measures put in place to protect the PII of Consumer Plaintiffs and the Class and the lack of efficacy of these security measures, Defendants' failure to timely and accurately disclose the Breach to Consumer Plaintiffs and the Class, and Defendants' continued acceptance of credit and debit card information as payment for goods after Defendants knew or should have known of the Breach's occurrence and before Defendants fixed the problems that allowed for the Breach and purged their systems of the malicious hacker software, constitute unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices . . . .

Furthermore, Plaintiffs and the other Class members would not have used their credit cards at Defendants' stores had they been informed of the deficient state of Defendants' cybersecurity. CAC ¶ 102. Defendants omitted these important facts and retained Plaintiffs' and Class members' money, even after they knew or should have known of the Data Breach's occurrence and their failure to achieve adequate remediation in its aftermath. Thus, reliance and causation are shown by the fact that Plaintiffs made purchases with their credit cards during the Data Breach.

Plaintiffs and Class members were acting reasonably when they relied upon Defendants, in the absence of any indication to the contrary, to undertake industry-mandated and otherwise reasonable measures to maintain the integrity and security of their payment-processing network. In addition, Defendants reaped substantial benefits by accepting payment cards as payment. And Defendants' violation of the consumer-protection laws resulted in the injuries set forth above. *See supra* Part

II.D.1. The CAC adequately pleaded claims under the state consumer-protection laws.

Defendants' conclusory assertions that certain elements of these claims are lacking must fail. The CAC contains more than enough factual matter, which, if proven, could sustain a verdict that Defendants violated state consumer-protection laws.

H. Plaintiffs State Claims Under the Data Breach-Notification Laws

Plaintiffs adequately stated claims on behalf of Plaintiffs and the Class under the data-breach-notification laws of Illinois, Maryland, and New Jersey. Defendants' attacks on these claims fail.

1. The Data-Breach-Notification Statutes of Illinois, Maryland, and New Jersey Provide Private Rights of Action

Illinois, Maryland, and New Jersey explicitly allow enforcement of their data-breach notice statutes through their respective state consumer-protection statutes. *See* 815 Ill. Comp. Stat. 530/20 (stating that violation of Illinois Personal Information Protection Act "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act"); 815 Ill. Comp. Stat. 505/10a (stating that "[a]ny person who suffers actual damage as a result of a violation of" the Consumer Fraud and Deceptive Business Practices Act may bring an action in

court against the violator);[11] Md. Code, Com. Law § 14-3508 (stating that violation of Maryland's Personal Information Protection Act is an "unfair or deceptive trade practice" under state's Consumer Protection Act, §13-101, *et seq.*); Md. Code, Com. Law §13-408 (stating that "any person may bring an action to recover for injury or loss sustained by him as the result of a [prohibited] practice");[12] N.J. Stat. § 56:8-166 (stating that "[i]t shall be an unlawful practice and a violation of [the Consumer Fraud Act] to willfully, knowingly or recklessly violate sections 10 through 13 of this amendatory and supplementary act"); N.J. Stat. § 56:8-19 ("Any person who suffers any ascertainable loss of moneys or property. . . as a result of the use or employment by another person of any method, act, or practice declared unlawful under [Consumer Fraud Act] . . . may bring an action . . . in any court of competent jurisdiction.");[13] *see also Target*, 66 F.Supp.3d at 1167 (concluding that

[11] *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 527–28 (N.D. Ill. 2011) (rejecting motion to dismiss as to PIPA claim, concluding that plaintiffs "state[d] a plausible claim" under Illinois Consumer Fraud Act "based on Michaels' alleged violation of PIPA").

[12] *See also Parks v. Alpharma*, 25 A.3d 200, 214 (Md. Ct. App. 2011) (stating that the Maryland Consumer Protection Act "provides a private civil remedy for consumers that can establish that they suffered 'actual injury or loss.'" (quoting *Citaramanis v. Hallowell*, 613 A.2d 964, 968–69 (Md. 1992)).

[13] *See also Weinberg v. Sprint Corp.*, 801 A.2d 281, 290 (N.J. 2002) (recognizing and explaining history of New Jersey Consumer Fraud Act's private right of action).

plaintiffs' data-breach claims in Illinois, Maryland, and New Jersey, among others, survived motion to dismiss).

Defendants' only authority to the contrary regarding these three states is an unpublished decision from the federal court in the Western District of Kentucky touching superficially on the New Jersey statute, stating that "[i]nsofar as the Court can tell, § 56:8–163 does not provide a private right of action for citizens to enforce its provisions." *Holmes v. Countrywide Fin. Corp.*, 2012 WL 2873892, at *13 (W.D. Ky. July 12, 2012). The court apparently overlooked the enforcement connection to the CFA in § 56:8–166, so *Holmes* is of little persuasive value. *See also Target*, 66 F. Supp. 3d at 1167 (confirming that New Jersey data-breach statute provides private right of action through CFA).

In addition, Plaintiffs may plead violations of data-breach-notification statutes and consumer-protection statutes, even if private enforcement of the former is done through the latter. *See Target*, 66 F. Supp. 3d at 1167 (denying motion to dismiss data-breach statutory claims as to six states that allow enforcement of data-breach statute through states' consumer-protection statutes). These are two different statutory claims, and Plaintiffs and the Class may prevail on one, both, or none; the fact that state legislators opted for enforcement of the data-breach statutes through consumer-protection statutes does not cause the data-breach notification cause of action to collapse or vanish into the consumer-

protection cause of action. If anything, it would limit the relief to which Plaintiffs are entitled, not the causes of action which Plaintiffs may plead.

2. Plaintiffs Sufficiently Allege Harm From Violation of the Data Breach Notification Statutes

Defendants next argue Plaintiffs failed to adequately plead harm from the delay in notification, because they do not separate harm from the delay from harm from the breach itself. Def. App. Br. 61. This too is wrong, as Plaintiffs adequately explain their injuries stemming both from the Data Breach itself and the delay in notification by Defendants. Plaintiffs have extensively explained why and how the breach caused them real injury and damages. *Supra* Part II.D.1.; *see also, e.g.*, *Allen*, 2015 WL 5076966 at *3 (finding allegation "that Plaintiffs have suffered and will continue to suffer financial losses caused by fraudulent charges to their compromised cards and bank fees associated with the data breach" to be sufficient to overcome motion to dismiss).

As a result of Defendants' unreasonable delay in providing notification, Plaintiffs were forced to spend more time and money in taking steps to refresh their recollections, contact their banks, seek out credit-card statements to ascertain their exposure to the increased risk of fraud created by the Data Breach, take additional steps to mitigate the risk of fraud, and to reduce the impact of post-Data Breach consequences. Were the notice not so unreasonably hampered, Plaintiffs would have more readily ascertained whether they were exposed to the risk (i.e.,

whether they used credit cards to purchase merchandise from Defendants during the Data Breach), and would have incurred less expense in making that determination. Importantly, Defendants only announced the Data Breach through public releases and not by individualized notice. CAC ¶ 11.

In addition, Defendants confused their customers by claiming the Data Breach was a series of unrelated incidents rather than the concerted and lengthy Data Breach that Plaintiffs allege took place. Nonetheless, Defendants' announcements invited, if not instructed, Plaintiffs to take measures to determine their exposure. As *Remijas* notes, "there are identifiable costs associated with the process of sorting things out." 794 F.3d at 692. That process begins with ascertaining the level of risk. Because the unreasonable delay in notification exacerbated Plaintiffs' costs, Plaintiffs sufficiently allege harm.

3. Plaintiffs Sufficiently Allege Defendants Violated the Data Breach Notification Statutes

The CAC, including Plaintiffs' specific causes of action under the state data-breach-notification statutes, alleges that Defendants unreasonably delayed notice of the Data Breach in violation of various data-breach-notification statutes. Defendants argue that Plaintiffs fail to sufficiently allege that Defendants had actual knowledge of the breach sufficient to trigger their duties and then delayed. Def. App. Br. 62–63.

In fact, Plaintiffs *did* allege that Defendants should have foreseen an intrusion and should have known about the intrusion earlier, so Defendants' argument fails. *See* CAC ¶¶ 46–61. Knowledge may be alleged generally, Fed. R. Civ. P. 9(b), and Plaintiffs have done so. *See* CAC ¶¶ 100–09, 122. In any event, Defendants' argument has nothing to do with the data-breach-notification statutory claims. The essence of the data-breach notice claim is that Defendants failed to provide timely and accurate notice under the statutes, preventing Plaintiffs from taking steps to mitigate the impact of the breach. CAC ¶¶ 107–17. These claims are more than adequately pleaded. Defendants cite no case law for the proposition that anything beyond these allegations is necessary.

Plaintiffs allege that Plaintiffs' PII was in fact stolen. CAC ¶¶ 8–9. This is assumed to be true for purposes of Defendants' motion to dismiss. Furthermore, each of the statutes at issue requires notification where the defendant reasonably believes that its database was accessed by unauthorized individuals or that its data has been acquired. *See* 815 Ill. Comp. Stat. 530/10(b) ("was, or is reasonably believed to have been, acquired by an unauthorized person"); N.J. Stat. 56:8-163(a) ("was, or is reasonably believed to have been, accessed by an unauthorized person"); Md. Code, Com. Law § 14-3504(c)(1) ("if it is likely that the breach has resulted or will result in" misuse of the personal information of a Maryland resident). Plaintiffs plausibly allege that Defendants knew or should have known

that the breach occurred, but nevertheless delayed in either remedying the breach or notifying the public that it had occurred. CAC ¶¶ 107–17.

Plaintiffs have adequately pleaded violations of all these standards, explaining why it is reasonable to believe not only that the data was accessed and acquired by unauthorized persons, and also that the data will be misused. CAC ¶¶ 60, 62–81. Defendants' own statements establish that the data was compromised. CAC ¶¶ 4–6, 36–37, 43–44. Plaintiffs have also pleaded that illicit web sites are selling the data. CAC ¶ 9. At this stage, this is all Plaintiffs are required to do, and this Court should deny Defendants' motion to dismiss.

I. Plaintiffs State Claims for Unjust Enrichment

Plaintiffs base their claims for unjust enrichment on two theories that a benefit was unjustly conveyed to Defendants. First, Plaintiffs argue that Defendants were unjustly enriched because Plaintiffs paid Defendants money for a level of network security that Defendants did not provide, despite being required to do so. Second, Plaintiffs argue that Defendants were unjustly enriched because Plaintiffs would have shopped elsewhere had they known of Defendants' deficient network security earlier. Defendants are incorrect to assert that these claims should be dismissed. Def. App. Br. 63–65.

To state a claim for unjust enrichment requires that Plaintiffs allege the following elements: (1) the plaintiff has conferred a benefit on the defendant; (2) the

defendant has knowledge of the benefit; (3) the defendant has accepted or retained the benefit conferred; and (4) the circumstances are such that it would be inequitable for the defendant to retain the benefit without paying fair value for it. *Resnick*, 693 F.3d at 1328. Across all jurisdictions, plaintiffs must plead that the defendant "knowingly received or obtained something of value which it in equity and good conscience should not have received." *Target*, 66 F. Supp. 3d at 1178 (internal quotation marks and alterations omitted).

Resnick v. AvMed supports the benefit of the bargain theory of harm, and this Court should adopt the Eleventh Circuit's reasoning. In *Resnick*, a corporation that delivered health-care services through health plans and government-sponsored managed-care plans was sued by its customers when two laptops containing customers' sensitive information were stolen from its offices. 693 F.3d at 1322. Among the plaintiffs' claims was a claim for unjust enrichment based on the defendant's retention of a portion of the plaintiffs' payments that allegedly ought to have been allocated to maintain adequate security over the confidential information compiled and kept by the defendant. The court held that this claim survived a motion to dismiss because the plaintiffs alleged that the defendant "appreciates or has knowledge of such benefit, that AvMed uses the premiums to pay for the administrative costs of data management and security, and that AvMed should not be permitted to retain the money belonging to Plaintiffs . . . because [AvMed] failed to

implement the data management and security measures that are mandated by industry standards." *Id.* at 1328 (internal quotations omitted).

Defendants charged cash customers and credit-card customers alike for the costs Defendants incur to maintain security over the currency exchanged in transactions with customers. Specifically, Defendants charge credit-card customers for adequate payment system network security to defray costs Defendants incur to implement sufficient electronic network security. Defendants, however, diverted those funds elsewhere and left their network security vulnerable to easily avoidable intrusions to their financial gain and to Plaintiffs' detriment. They did this because, *inter alia*, unlike with cash customers, the customers initially bear all the risk of criminal intrusions to a payment-processing network.

As in *Resnick*, Defendants ought not to retain these diverted funds because Plaintiffs' and the other Class members' Private Information is now in the hands of cybercriminals intent on misusing and already actively engaged in misusing the data for their own gain. In equity and good conscience, Defendants ought not to retain those diverted funds that were intended to, but did not, provide adequate and industry-mandated network security to Plaintiffs and the other Class members.

Furthermore, Plaintiffs adequately pleaded unjust enrichment under the theory that they would have shopped elsewhere had they known about Defendants' deficient data security practices. The *Target* court implicitly upheld, at the pleading stage, the

claims by similar plaintiffs who alleged they would not have shopped at Target or would have used alternative methods of payment. *Target*, 66 F. Supp. 3d at 1178. Plaintiffs here also allege that they would not have shopped or would have used alternative methods of payment had they been aware of the data-security deficiencies. *See* CAC ¶¶ 118, 156–57. Thus, Plaintiffs have properly pleaded a claim for unjust enrichment.

Defendants' argument that Plaintiffs pleaded facts negating this theory of harm is flawed. First, Plaintiffs maintain that the first and second data-breach notifications relate to one overarching Data Breach, so the post-breach transactions are not in issue. *See* CAC ¶ 7. However, even if the two occurrences were unrelated, the first data breach announcement did not absolve Defendants of their responsibility to secure their networks going forward, and Plaintiffs were entitled to rely on Defendants (especially in the sobering aftermath of the first data breach) to implement security measures that would avert a second data breach. The fact that Defendants continued to accept credit-card payments as Level 1 merchants implied their ability to comply with requirements. In addition, all reasonable inferences are to be resolved in favor of Plaintiffs. Plaintiffs sufficiently pleaded harm for persons who shopped at Defendants' stores after the first data breach announcement.

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that this Court reverse the January 7, 2016 Order and Judgment of the district court, find in favor of Plaintiffs with respect to Defendants' cross-appeal, should the Court address it, and remand this case to the district court for further proceedings.

Dated: September 14, 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 P.L.L.P.
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 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 has been scanned for computer viruses and are virus free.

September 14, 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 September 14, 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.

September 14, 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 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 12,941 words, including headings, footnotes, and quotations.

September 14, 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