

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MINNESOTA**

IN RE: SuperValu, Inc., Customer Data  
Security Breach Litigation

**MEMORANDUM OPINION  
AND ORDER**

Court File No. 14-MD-2586 ADM/TNL

This Document Relates to:  
All Actions

---

Ben Barnow, Esq., Barnow and Associates, P.C., Chicago, IL; Edwin J. Kilpela, Jr., Esq., Carlson Lynch Sweet & Kilpela, LLP, Pittsburgh, PA; Rhett A. McSweeney, Esq., McSweeney/Langevin, LLC, Minneapolis, MN; Karen Hanson Riebel, Esq., and Richard A. Lockridge, Esq., Lockridge Grindal Nauen P.L.L.P., Minneapolis, MN, on behalf of Plaintiffs.

Harvey J. Wolkoff, Esq., and Kathryn E. Wilhelm, Esq., Ropes & Gray LLP, Boston, MA; Katherine S. Barrett Wiik, Esq., and Stephen P. Safranski, Esq., Robins Kaplan LLP, Minneapolis, MN, on behalf of Defendant SuperValu, Inc.

John L. Landolfi, Esq., Vorys, Sater, Seymour and Pease LLP, Columbus, OH; and Marc A. Al, Esq., Stoel Rives LLP, Minneapolis, MN, on behalf of Defendants AB Acquisition, LLC and New Albertson's Inc.

---

**I. INTRODUCTION**

On November 3, 2015, the undersigned United States District Judge heard oral argument on Defendants SuperValu, Inc. ("SuperValu"), AB Acquisition, LLC ("AB Acquisition"), and New Albertson's Inc.'s ("Albertson's") (collectively, "Defendants") Motion to Dismiss Plaintiffs' Consolidated Amended Class Action Complaint [Docket No. 33]. For the reasons set forth below, the Motion is granted.

**II. BACKGROUND**

In this multidistrict litigation case, sixteen named plaintiffs ("Plaintiffs") allege they were harmed by hackers gaining access to and installing malicious software on the payment-processing network for payment card transactions at Defendants' retail grocery stores.

Consolidated Am. Class Action Compl. (“Amended Complaint”) [Docket No. 28] ¶¶ 16–45. Plaintiffs allege the malicious software released and disclosed the Personal Identifying Information (“PII”) of Plaintiffs and Class Members who used their payment cards for purchases at the affected stores. Id. ¶ 36. The Amended Complaint states claims for negligence, negligence per se, breach of implied contract, unjust enrichment, and violations of various state consumer protection and data breach notification laws. Id. ¶¶ 13, 96–159. Plaintiffs assert their claims as class actions. Id. ¶¶ 83–95.

### **A. Defendants**

Defendants own and operate retail grocery stores in the United States. Id. ¶¶ 2-3, 33-35. SuperValu controls the payment processing at its stores and also provides payment processing services for AB Acquisition and Albertson’s stores. Id. ¶ 3.

### **B. Data Breach**

On August 14, 2014, Defendants announced in press releases that from June 22, 2014 to July 17, 2014, hackers had gained unauthorized access to and installed malicious software on the portion of SuperValu’s computer network that processes payment card transactions for Defendants’ retail stores. Id. ¶¶ 4–5, 36. The intrusion resulted in potential theft of information embedded in the magnetic strip of payment cards for sales transacted at 209 SuperValu stores and 836 AB Acquisition stores. Id. ¶ 36. The PII embedded in the magnetic strip included cardholder names, account numbers, expiration dates, and PINS. Id. ¶¶ 1, 42. The press releases stated Defendants’ offer of 12 months of complimentary consumer identity protection services to customers whose cards may have been affected by the data breach. Id. ¶ 45.

On September 29, 2014, Defendants announced in press releases that a second data

breach occurred in late August or early September 2014. Id. ¶ 6. In this second instance, hackers installed different malware onto the portion of SuperValu’s computer network that processes payment card transactions for some retail stores owned or operated by AB Acquisition and Albertson’s (collectively referred to with the stores affected in the first breach as the “Affected Stores”). Id. ¶¶ 6, 44. Plaintiffs allege the two incidents (collectively referred to as the “Data Breach”) are related and stem from Defendants’ same fundamental security failures. Id. ¶ 7.

### **C. Named Plaintiffs**

Plaintiffs are consumers who shopped at Defendants’ stores that were affected by the Data Breach. Id. ¶¶ 16–31. Plaintiffs provided their PII to Defendants when they used their payment cards at Defendants’ Affected Stores. Id. ¶¶ 1, 16–31.

### **D. Alleged Harm**

Although customer data at over 1,000 of Defendants’ stores was accessed, the only alleged misuse of any Plaintiff’s PII following the Data Breach is a single unauthorized charge on one Plaintiff’s credit card. Plaintiff David Holmes alleges he experienced a fraudulent charge on his payment card after shopping at one of Defendants’ Affected Stores and, upon noticing the fraudulent charge on his credit card statement, he immediately cancelled his credit card.<sup>1</sup> Id. ¶ 31. Holmes does not specify the amount or date of the fraudulent charge, nor does he allege the charge was unreimbursed or that he incurred bank fees or other monetary losses related to the charge. See id. No other Plaintiff alleges any unauthorized charges on their account, and no

---

<sup>1</sup> Holmes does not specify whether he shopped at an Affected Store during the time periods associated with the Data Breach. See id. ¶ 31. For the purposes of this Motion, the Court assumes he did.

Plaintiff, including Holmes, has alleged experiencing identity theft or attempted identity theft after the Data Breach. See generally Am. Compl.

All sixteen of the named Plaintiffs allege that after Defendants announced the Data Breach, Plaintiffs spent time determining whether their cards were compromised and monitoring their account information to guard against potential fraud. Id. ¶¶ 16–31. One Plaintiff, Kenneth Hanff, further alleges he closed his checking account and opened a new one to prevent fraudulent purchases. Id. ¶ 18.

Based on these factual allegations, Plaintiffs allege that Defendants’ wrongful conduct, the resulting Data Breach, and the potential disclosure of Plaintiffs’ and other Class Members’ PII have caused them to suffer harm including: (i) diminished value of their PII; (ii) untimely and inadequate notification of the Data Breach; (iii) increased risk of future losses, economic damages, and other harm; (iv) opportunity cost and value of lost time spent monitoring financial accounts and payment card accounts; (v) invasion of privacy and breach of the confidentiality of their PII by Defendants’ unauthorized release and disclosure; and (vi) lost benefit of the bargain. Id. ¶¶ 32, 82.

### **E. Procedural History**

A total of four putative class actions brought by a total of twelve Plaintiffs were filed against Defendants in federal courts in Illinois, Minnesota, and Idaho. See, McPeak v. SuperValu, Inc., 3:14-cv-00899 (S.D. Ill., filed Aug. 18, 2014); Hanff v. SuperValu Inc., 14-cv-3252 (D. Minn., filed Aug. 25, 2014); Mertz v. SuperValu, Inc., 14-cv-04660 (D. Minn., filed Nov. 4, 2014); and Rocke v. SuperValu, Inc., 1:14-cv-00511 (D. Idaho, filed Nov. 26, 2014). In December 2014, the Judicial Panel on Multidistrict Litigation centralized the four complaints to

this Court for coordinated pre-trial proceedings. See Transfer Order [Docket No. 1].

On June 26, 2015, Plaintiffs filed the Amended Complaint alleging six causes of action on behalf of sixteen named Plaintiffs. See generally Am. Compl. The sixteen named Plaintiffs consist of the twelve original Plaintiffs plus four new Plaintiffs. See id. ¶¶ 27–30.

Defendants now move to dismiss the Amended Complaint for lack of subject matter jurisdiction under Rule 12(b)(1) and for failure to state a claim under Rule 12(b)(6).

### **III. DISCUSSION**

#### **A. Rule 12(b)(1): Lack of Subject Matter Jurisdiction**

Defendants argue the Amended Complaint must be dismissed under Rule 12(b)(1) for Plaintiffs’ failure to allege facts establishing Article III standing, which is a prerequisite to subject matter jurisdiction. See Lujan v. Defenders of Wildlife, 504 U.S. 555, 559–60 (1992).

##### **1. Standard of Review**

Defendants’ Motion attacks the sufficiency of the pleadings and thus raises a facial, rather than factual, challenge to the Court’s subject matter jurisdiction. See Stalley v. Catholic Health Initiatives, 509 F.3d 517, 521 (8th Cir. 2007). In analyzing a facial challenge to jurisdiction, the Court applies the same standard of review as that in Rule 12 (b)(6) cases. Id. The Court “accepts as true all factual allegations in the complaint, giving no effect to conclusory allegations of law.” Id. Plaintiffs must affirmatively and plausibly assert facts that suggest they have the right to jurisdiction, rather than facts that are merely consistent with that right. See id. (citing Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007)). “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 v. Palm, 621 F.3d 816, 818 (8th Cir. 2010) (quoting

Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)).

## **2. Article III Standing**

“Article III standing is a threshold question in every federal court case.” United States v. One Lincoln Navigator 1998, 328 F.3d 1011, 1013 (8th Cir. 2003). The party invoking federal jurisdiction has the burden of establishing standing. Lujan, 504 U.S. at 560. To meet this burden, a plaintiff must show: (1) an injury in fact; (2) a causal connection between the injury and the challenged conduct of the defendant; and (3) a likelihood that a favorable ruling will redress the alleged injury. Young Am. Corp. v. Affiliated Computer Servs. (ACS), Inc., 424 F.3d 840, 843 (8th Cir. 2005) (citing Lujan, 504 U.S. at 560–61). Each element “must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation.” Lujan, 504 U.S. at 561.

To satisfy the injury in fact element of standing, an injury must be “concrete, particularized, and actual or imminent.” Clapper v. Amnesty Int’l USA, 133 S.Ct. 1138, 1147 (2013). When a party’s alleged injury is based on future harm, standing exists if the threatened injury is “‘certainly impending,’ or there is a ‘substantial risk’ that the harm will occur.” Susan B. Anthony List v. Driehaus, 134 S.Ct. 2334, 2341 (2014) (quoting Clapper, 133 S.Ct. at 1147, 1150 n.5). “[A]llegations of possible future injury are not sufficient.” Clapper, 133 S.Ct. at 1147 (internal quotation marks omitted) (emphasis in original).

The requirement that a future injury be imminent “ensure[s] that the alleged injury is not too speculative for Article III purposes.” Lujan, 504 U.S. at 564 n.2. Although imminence is a “somewhat elastic concept,” it requires “that the injury proceed with a high degree of

immediacy, so as to reduce the possibility of deciding a case in which no injury would have occurred at all.” Id. Additionally, where a threatened injury hinges on speculation about the actions of third parties, standing is less likely to exist. See Clapper, 133 S.Ct. at 1150 (expressing “reluctance to endorse standing theories that rest on speculation about the decisions of independent actors”); id. at 1150 n.5 (“Plaintiffs cannot rely on speculation about the unfettered choices made by independent actors not before the court.”) (internal quotations omitted).

In a class action lawsuit, “named plaintiffs who represent a class must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.” Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 40 n.20 (1976). “[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class.” O’Shea v. Littleton, 414 U.S. 488, 494 (1974) (internal quotations omitted).

The Amended Complaint alleges several forms of injury: (a) increased risk of future losses, economic damages and other harm; (b) opportunity cost and value of lost time spent monitoring financial accounts and payment card accounts; (c) diminished value of Plaintiffs’ PII; (d) untimely and inadequate notification of the Data Breach; (e) invasion of privacy and breach of the confidentiality of Plaintiffs’ PII due to Defendants’ unauthorized release and disclosure; and (f) lost benefit of the bargain. See Am. Compl. ¶¶ 32, 82. Defendants argue Plaintiffs have failed to plausibly allege injury that is “concrete, particularized, and actual or imminent.” Clapper, 133 S.Ct. at 1147.

**a. Increased Risk of Future Harm**

Plaintiffs allege they face a substantial risk of future harm because Defendants' failure to properly secure their computer network has allowed hackers to steal their PII for fraudulent use. See Am. Compl. ¶ 8 (“Defendants’ security failures enabled the hackers to steal Consumer Plaintiffs’ and the other Class members’ PII . . . and put Consumer Plaintiffs’ and the other Class members’ financial information at serious, immediate, and ongoing risk.”); id. ¶ 9 (“On information and belief, illicit websites are selling the stolen payment card PII ‘dumps’ to international card counterfeiters and fraudsters . . . .”). Defendants argue that Plaintiffs’ allegations of future harm are actually only speculative claims of possible future injury, which are not sufficient to satisfy Article III standing.

In data security breach cases where plaintiffs’ data has not been misused following the breach, the vast majority of courts have held that the risk of future identity theft or fraud is too speculative to constitute an injury in fact for purposes of Article III standing. See, e.g., Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) (“Most courts have held that such plaintiffs lack standing because the harm is too speculative. We agree with the holdings in those cases.”) (internal citations omitted); In re Zappos.com, Inc. Customer Data Sec. Breach Litig., ----F. Supp. 3d ---, No. 12-00325, 2015 WL 3466943, at \*5 (D. Nev. June 1, 2015) (“The majority of courts dealing with data-breach cases post-Clapper have held that absent allegations of actual identity theft or other fraud, the increased risk of such harm alone is insufficient to satisfy Article III standing.”); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 654–56 (S.D. Ohio 2014); Green v. eBay, Inc., No. 14-1688, 2015 WL 2066531, at \*3 n.33 (E.D. La. May 4, 2015) (listing cases); Whalen v. Michael Stores, Inc., No. 14-7006, 2015 WL 9462108, at \*4–\*5

(E.D.N.Y. Dec. 28, 2015); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 876–77 (N.D. Ill. 2014); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 364–68 (M.D. Pa. 2015); Lewert v. P.F. Chang’s China Bistro, Inc., No. 14-4787, 2014 WL 7005097, at \*3 (N.D. Ill. Dec. 10, 2014).

The speculative nature of the threatened injury stems from the numerous variables upon which the future harm depends, including whether the hacker: (1) read, copied, and understood [Plaintiffs’] personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [Plaintiffs] by making unauthorized transactions in [Plaintiffs’] names.” Reilly, 664 F.3d at 42; see also Strautins, 27 F. Supp. 3d at 876 (holding plaintiff failed to plausibly allege an “imminent” or “certainly impending” risk of identity theft where the threatened harm depended on “whether [plaintiff and class members’] data was actually taken during the breach, whether it was subsequently sold or otherwise transferred, whether anyone who obtained the data attempted to use it, and whether or not they succeeded”); Galaria, 998 F. Supp. 2d at 655 (“[W]hether Named Plaintiffs will become victims of theft or fraud . . . is entirely contingent on what, if anything, the third party criminals do with that information.”); In re Zappos.com, 2015 WL 3466943, at \*8 (finding future harm depended upon the capabilities and decisions of the person in possession of plaintiffs’ data); Green, 2015 WL 2066531, at \*5 (holding that several variables caused harm to be “far too hypothetical” for Article III standing). In addition to the speculation of whether future harm from a data security breach will materialize, it cannot be known when such harm will occur. As more time lapses without the threatened injury actually occurring, the notion that the harm is imminent becomes less likely. In re Zappos.com, 2015 WL 3466943 at \*8; Storm, 90 F. Supp.

3d at 367.

Here, the Data Breach of Defendants' computer network affected more than 1,000 retail grocery stores and occurred nearly one and a half years ago. Despite the large number of Affected Stores and the significant amount of time that has elapsed, the only facts asserted that any of Plaintiffs' PII has been misused is the single incident alleged by Plaintiff Holmes. Holmes noticed a single unauthorized charge (of an unspecified amount on an unspecified date) on his credit card statement after learning of the Data Breach. See Am. Compl. ¶ 31. Given 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. Thus, the isolated single instance of an unauthorized charge is not indicative of data misuse that is fairly traceable to the Data Breach. See, e.g., In re Barnes & Noble Pin Pad Litig., No. 12-8617, 2013 WL 4759588, at \*6 (N.D. Ill. Sept. 3, 2013) (“[I]t is not directly apparent that the fraudulent charge was in any way related to the security breach at Barnes & Noble.”).

Based on the absence of any other allegations that Plaintiffs' PII has been misused, the Court is left to speculate about whether the hackers who gained access to Defendants' payment processing network were able to capture or steal Plaintiffs' PII;<sup>2</sup> whether the hackers or other

---

<sup>2</sup> The Amended Complaint asserts that Plaintiffs' PII was disclosed to the hackers during the Data Breach and that the criminals were able to “steal” or “harvest” the PII for their illicit use. See, e.g., Am. Compl. ¶¶ 4, 8, 36, 40, 44. These allegations are largely based on Defendants' August and September 2014 press releases, which are referenced in the Amended Complaint and thus properly considered here. See, e.g., id. ¶¶ 4–6, 36–37, 44 (referencing Defendants' announcements about Data Breach); Moses.com Sec., Inc. v. Comprehensive Software Sys., Inc., 406 F.3d 1052, 1063 n.3 (8th Cir. 2005) (stating press release could be

criminals will attempt to use the PII; and whether those attempts will be successful. See Reilly, 664 F.3d at 45 (“Any damages that may occur here are entirely speculative and dependent on the skill and intent of the hacker.”). This speculation prevents the Court from finding an increased risk of fraud and identity theft is “certainly impending” or that there is a “substantial risk” the harm will occur. Clapper, 133 S.Ct. at 1147, 1150 n.5. Moreover, the passage of nearly a year and a half without the occurrence of harm traceable to the Data Breach makes it unlikely that such threatened harm is imminent. As one court has observed:

Determining what the lapsed time means . . . requires the Court to engage in speculation—precisely what the Supreme Court has counseled against. Clapper, 133 S.Ct. at 1149–50 (refusing standing based on speculation). It could signify that Plaintiffs are in the clear, meaning that the data obtained by the hacker was not useful in effectuating acts of theft or fraud. Or it could mean that the hacker is simply sitting on the information until the time is “right,” which could be a few more years down the road. Or the lapsed time might mean a number of other scenarios. It is simply unclear.

In re Zappos.com, 2015 WL 3466943, at \*7. Therefore, Plaintiffs’ allegations of future harm do not satisfy the injury-in-fact requirement for Article III standing.

The recent cases relied on by Plaintiffs do not compel a different result. Those cases included factual allegations of substantial data misuse which plausibly suggested that the hackers

---

considered on motion to dismiss because it was referenced in complaint and thus incorporated into pleadings). However, Defendants’ press releases explicitly state there has been no determination that customer data was stolen by the intruder. See Wolkoff Decl. [Docket No. 36] Exs. A–D. A hacker’s ability to gain access to a computer network does not necessarily equate to the ability to read, copy, or otherwise steal data. See, e.g., Green, 2015 WL 2066531, at \*5 (“Whether Plaintiff and other class members actually become victims of identity theft depends on numerous variables, including whether their data was actually taken when it was accessed . . . .”); Reilly, 664 F.3d at 42 (stating that future harm from a data breach depends in part on whether the hacker “read, copied, and understood [the plaintiffs’] personal information”). Here, no widespread data misuse has been alleged that would suggest the hackers were successful in stealing Plaintiffs’ and Class Members’ PII or that they are now able to use it for illicit purposes.

had succeeded in stealing the data and were willing and able to use it for future theft or fraud. See Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692–94 (7th Cir. 2015); In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215–16 (N.D. Cal. 2014); Corona v. Sony Pictures Enter., No. 14-09600, 2015 WL 3916744, at \*3 (C.D. Cal. June 15, 2015); In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014).

For example, in Remijas, more than 9,200 customers experienced fraudulent charges on their payment cards within six months after a data breach occurred at Neiman Marcus. Remijas, 794 F.3d at 690. Based on the widespread misuse of customers’ payment card data, there was “no need to speculate” as to whether the customers’ information had been stolen. Id. at 693. Given that hackers had already successfully used customers’ data to incur fraudulent charges, the court concluded that Neiman Marcus customers should not have to wait until they were victimized by identity theft or credit card fraud to obtain standing, because there was an objectively reasonable likelihood that such an injury would occur. Id. Similarly in Adobe, speculation as to whether the hackers had stolen the data and intended to use it was not necessary, because some of Adobe’s stolen data had already surfaced on the internet.<sup>3</sup> In re Adobe, 66 F. Supp. 3d at 1216. Significant data misuse was also alleged in Corona, where

---

<sup>3</sup> Although Plaintiffs in this case allege that illicit websites are selling Plaintiffs’ PII to counterfeiters and fraudsters, the allegation is made “[o]n information and belief.” Am. Compl. ¶ 9. Plaintiffs argue that the Twombly plausibility standard does not prevent them from pleading facts alleged “upon information and belief” where the facts are peculiarly within Defendants’ possession and control or where the belief is based on factual information that makes the inference plausible. Pls.’ Mem. Opp’n [Docket No. 40] 25–26 (citing Artista Records, LLC v. Doe 3, 604 F.3d 110, 120 (2d Cir. 2010)). However, the facts of third parties’ use of Plaintiffs’ PII are not peculiarly within Defendants’ possession and control. For example, Plaintiffs can learn of criminal activity through review of their account statements or contact with their banks. Additionally, Plaintiffs and Defendants are on equal footing in discovering the identity of a website or virtual marketplace where Plaintiffs’ PII is being sold.

several Sony employees received threatening messages from hackers demanding that the employees release even more of their PII, and some plaintiffs had experienced attempted identity theft. Corona, 2015 WL 3916744, at \*3–\*4. Likewise in Target, many of the 114 named Plaintiffs alleged that they actually incurred unauthorized charges; lost access to their accounts; and/or were forced to pay late fees, card-replacement fees, and credit monitoring costs because the hackers misused their personal information. In re Target, 66 F. Supp. 3d at 1158. Based on these allegations, the Target court concluded that plaintiffs had plausibly alleged standing. See id. at 1159. Future harm was not addressed. See id.

These cases alleging widespread data misuse contrast sharply with the allegations made in the instant case. Here, only one unauthorized credit card charge (of an unspecified date and amount) is alleged to have occurred in the fifteen-month time period following the Data Breach that affected over 1,000 of Defendants’ stores. This singular incident from one named Plaintiff over the course of more than a year following the Data Breach is not sufficient to “nudge[]” Plaintiffs’ class claims of data misuse or imminent misuse “across the line from conceivable to plausible.” Twombly, 550 U.S. at 570. Thus, Plaintiffs have failed to allege sufficient facts to show that future harm from the Data Breach is “certainly impending” or that there is a “substantial risk that the harm will occur.” Clapper, 133 S.Ct. at 1147, 1150 n.5.

#### **b. Opportunity and Mitigation Costs**

Plaintiffs allege they have suffered harm based on mitigation costs, including time spent monitoring their account information to guard against potential fraud and, in the case of Plaintiff Hanff, costs and expenses associated with opening a new checking account. As the Supreme Court has recently explained, plaintiffs “cannot manufacture standing merely by inflicting harm

on themselves based on their fears of hypothetical future harm that is not certainly impending.” Clapper, 133 S.Ct. at 1151. “If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.” Id. In data breach cases, courts consistently hold that the cost to mitigate the risk of future harm does not constitute an injury in fact unless the future harm being mitigated against is itself imminent. See, e.g., In re Adobe, 66 F. Supp. 3d at 1217; In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C. 2014); In re Zappos.com, 2015 WL 3466943, at \*10; Lewert, 2014 WL 7005097, at \*3. Here, the risk of future harm being mitigated against is not imminent. Thus, the cost to mitigate the risk is not a sufficient injury in fact to confer Article III standing.

### **c. Diminished Value of Plaintiffs’ Payment Card PII**

Plaintiffs also allege that the value of their PII was lost or diminished as result of the Data Breach. Assuming without deciding that Plaintiffs’ PII had monetary value, Plaintiffs have failed to allege any facts explaining how their PII became less valuable as a result of the Data Breach. Plaintiffs have not alleged that they tried to sell their PII but were not able to do so or were forced to accept a lower price. Therefore, Plaintiffs have not alleged an injury in fact under this theory. See In re Zappos.com, 2015 WL 3466943, at \*3 (finding no injury in fact where plaintiffs had not alleged that the data breach had prevented them from selling their personal information at the price it was worth); In re SAIC, 45 F. Supp. 3d at 30 (same); Galaria, 998 F. Supp. 2d at 660 (same); Green, 2015 WL 2066531, at \*5 n.59 (“Even if the Court were to find that personal information has an inherent value and the deprivation of such value is an injury sufficient to confer standing, Plaintiff has failed to allege facts indicating how the value of his

personal information has decreased as a result of the Data Breach.”).

**d. Delayed or Inadequate Notification**

Plaintiffs further allege they were harmed by Defendants’ “untimely and inadequate notification of the Data Breach.” Am. Compl. ¶ 82. Plaintiffs argue the delayed notification forced them to spend more time and money to: (1) refresh their recollections, contact their banks, and locate their credit card statements to determine whether they had been exposed to the risk of fraud created by the Data Breach; and (2) take additional steps to mitigate the risk of fraud. Plaintiffs thus contend they have standing to assert claims under state data breach notification laws that grant a private right of action. These assertions of increased mitigation costs due to delayed notification are not alleged in the Amended Complaint. Even if they had been, the allegations would not have established Article III standing because as discussed above, the cost to mitigate the risk of future harm does not constitute an injury in fact unless the risk of future harm is imminent. “Plaintiffs must plead an injury beyond a statutory violation to meet the standing requirement of Article III.” In re Barnes & Noble, 2013 WL 4759588, at \*3. Therefore, “[e]ven assuming the statutes have been violated by the delay or inadequacy of [Defendants’] notification, breach of these statutes is insufficient to establish standing without any actual damages due to the breach.” Id.

**e. Invasion of Privacy and Breach of Confidentiality**

Plaintiffs also allege they suffered an invasion of privacy and breach of confidentiality of their PII as a result of the Data Breach. However, Plaintiffs have not alleged facts showing that the loss of privacy and confidentiality resulted in a concrete injury. Therefore, this theory of standing also fails. See In re Zappos.com, 2015 WL 3466943, at \*11 n.5 (finding no Article III

standing under a loss of privacy theory because plaintiffs “failed to show how that loss amounts to a concrete and particularized injury”).

**f. Lost Benefit of Bargain**

Finally, Plaintiffs allege they were harmed by the lost benefit of their bargain. Am. Compl. ¶ 32. This theory is consistently rejected in data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach. See, e.g., In re Zappos.com, 2015 WL 3466943, at \*11 n.5 (rejecting benefit-of-bargain theory where plaintiffs had not explained how the data breach impacted the value of the goods they purchased, and further had not alleged facts showing that the price plaintiffs paid for such goods incorporated a sum that both parties understood would be allocated towards the protection of customer data); Fernandez v. Leidos, Inc., --- F. Supp. 3d ---, No. 14-02247, 2015 WL 5095893, at \*9 (E.D. Cal. Aug. 28, 2015) (finding no standing where plaintiff failed to allege facts from which a plausible inference could be drawn that the value of plaintiff’s health care and insurance coverage had been diminished as a result of the data breach); Remijas, 794 F.3d at 694–95 (noting in dicta that the benefit-of-the-bargain theory was “problematic” and “dubious” where plaintiffs had not alleged any defect in any product they had purchased).

Here, Plaintiffs do not allege that the Data Breach diminished the value of the groceries or other goods they purchased from Defendants. Nor do Plaintiffs allege facts showing that the price they paid for the goods included an amount that both parties understood would be allocated toward protecting customer data. Thus, Plaintiffs have not alleged a cognizable injury based on the lost benefit of their bargain.

### **3. Dismissal Without Prejudice**

Based on Plaintiffs' failure to plead specific facts to demonstrate they have standing to bring this suit, this case must be dismissed. Because the dismissal is for lack of standing under Rule 12(b)(1), the dismissal is without prejudice. See, e.g., Storm, 90 F. Supp. 3d at 369 (dismissing case without prejudice for lack of standing under Rule 12(b)(1)); In re Zappos.com, 2015 WL 3466943, at \*11 (same).

### **B. Failure to State a Claim**

Because the Court concludes that Plaintiffs lack standing under Article III, the Court is without subject matter jurisdiction to determine whether the Amended Complaint states a claim for relief under Rule 12(b)(6).

## **IV. CONCLUSION**

Based upon the foregoing, and all the files, records, and proceedings herein, **IT IS HEREBY ORDERED** that Defendants' Motion to Dismiss Plaintiffs' Consolidated Amended Class Action Complaint [Docket No. 33] is **GRANTED**. The Consolidated Amended Class Action Complaint is dismissed without prejudice.

**LET JUDGMENT BE ENTERED ACCORDINGLY.**

BY THE COURT:

s/Ann D. Montgomery  
ANN D. MONTGOMERY  
U.S. DISTRICT JUDGE

Dated: January 7, 2016.