

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MINNESOTA

KENNETH HANFF, IVANKA SOLDAN,  
RIFET BOSNJAK, MELISSA ALLERUZZO,  
and CAROL PUCKETT, individually and on  
behalf of all others similarly situated,

Plaintiffs,

v.

SUPERVALU INC., a Minnesota  
Corporation,

Defendant.

CASE NO:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

**CLASS ACTION COMPLAINT**

Plaintiffs, Kenneth Hanff, Ivanka Soldan, Rifet Bosnjak, Melissa Alleruzzo, and Carol Puckett (“Plaintiffs”), individually and on behalf of all others similarly situated, by and through their attorneys, upon personal knowledge as to facts pertaining to them and information and belief as to all other matters, bring this Class Action Complaint against defendant Supervalu Inc. (“Defendant” or “Supervalu”).

**NATURE OF THE ACTION**

1. Plaintiffs bring this class action against Supervalu for its failure to secure and safeguard the personal financial data—including, but not limited to, name, account numbers, expiration dates, PINs, and other numerical information (collectively, “Personal identifying information” or “PII”)—of individuals who shopped at its retail stores, including Cub Foods, Farm Fresh, Hornbacher’s, Shop ‘n Save, and Shoppers Food & Pharmacy, and franchise Cub Foods stores, as well as Albertsons, ACME Markets, Jewel-Osco, Shaw’s and Star Markets retail stores that Supervalu sold in 2013 but for which it provided and still provides payment card

processing services (collectively referred to hereinafter as the “Concerned Stores”).

2. On or about August 14, 2014, Supervalu announced that it experienced a criminal intrusion into the portion of its computer network that processes payment card transactions for its retail stores, including Cub Foods, Farm Fresh, Hornbacher’s, Shop ‘n Save, and Shoppers Food & Pharmacy, and franchise Cub Foods stores.

3. According to the announcement, attached hereto as Exhibit 1, between June 22 and July 17, 2014—nearly an entire month—the cardholder data of customers shopping at 209 Supervalu-owned retail stores and franchisee stores nationwide was being stolen by the intruders.

4. Defendant provides payment card processing for certain retail stores it previously owned, including but not limited to Albertsons, ACME Markets, Jewel-Osco, and Shaw’s and Star Markets. Defendant sold these retail stores to AB Acquisitions LLC in 2013. On August 14, 2014, AB Acquisition likewise announced that an unlawful intrusion may have affected its stores throughout the country, in California, Idaho, Montana, North Dakota, Nevada, Oregon, Utah, Washington, Wyoming, Pennsylvania, Maryland, Delaware, New Jersey, Iowa, Illinois, Indiana, Maine, Massachusetts, Vermont, New Hampshire, and Rhode Island. According to Defendant, the two intrusions are related and took place over the same time period, June 22–July 17, 2014. The intrusions will be referred to hereinafter collectively as the “Data Breach.”

5. Defendant’s security failures enabled the hackers to steal Plaintiffs’ and the other Class members’ PII from within Defendant’s computer systems and put Plaintiffs’ and the other Class members’ financial information at serious, immediate, and ongoing risk. The practice with such data breaches is that hackers will continue to use the information they obtained as a result of inadequate security, as with Defendant here, to exploit and injure consumers by selling the PII to third parties and otherwise using the PII for illicit purposes. That activity now blankets the

Plaintiffs and the other Class members with a known and documented risk.

6. The Data Breach was caused and enabled by Defendant's violation of its obligations to abide by best practices and industry standards concerning the security of its computer and payment processing systems. Defendant failed to comply with security standards and allowed its customers' PII to be compromised by cutting corners on security measures that could have prevented or mitigated the Data Breach. Defendant's failure to monitor who accessed its networks and Plaintiffs' and the other Class members' PII resulted in unauthorized individuals gaining access to its networks continuously for nearly an entire month.

7. Defendant also failed to timely disclose the extent of the Data Breach, failed to individually notify each of the affected individuals of the Data Breach in a timely manner, and failed to take other reasonable steps to clearly and conspicuously inform Plaintiffs and the other Class members of the nature and extent of the Data Breach. By failing to provide adequate notice, Defendant prevented Plaintiffs and the other Class members from protecting themselves from the consequences of the Data Breach. Many affected customers will first learn that their PII had been stolen only after being notified of fraudulent activity on their accounts, being wrongfully denied credit, or receiving an inordinate amount of spam e-mails and other intrusions into their privacy.

8. Accordingly, Plaintiffs, individually and on behalf of other members of the Class, assert claims for breach of implied contract, negligence, violation of the Minnesota Deceptive Trade Practices Act, Minn. Stat. Ann. § 325D.43, *et. seq.*, invasion of privacy, and seek injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief authorized in equity or by law.

**JURISDICTION AND VENUE**

9. The Court has jurisdiction over Plaintiffs' claims pursuant to 28 U.S.C. § 1332(d), because this matter was brought as a class action under Fed. R. Civ. P. 23, at least one proposed Class member is of diverse citizenship from Defendant, the proposed Class includes more than 100 members, and the aggregate amount in controversy exceeds five million dollars (\$5,000,000.00), excluding interest and costs.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1391, because Defendant resides in this District and committed the wrongful conduct against Class members in this district.

**PARTIES**

11. Plaintiff Kenneth Hanff is a resident of Missouri. He shopped at the Defendant-owned Shop 'N Save located at 60 Harvester Square in St. Charles, Missouri on June 23, July 2, July 10, July 14, and July 16, 2014. For each of these visits, Hanff used a debit card to pay for his merchandise. The PII on his debit card was compromised by the Data Breach. Hanff has suffered and will continue to suffer losses and damages as a result of the Data Breach.

12. Plaintiff Ivanka Soldan is a resident of Missouri. She shopped at the Defendant-owned Shop 'n Save located at 1253 Water Tower Place in Arnold, Missouri on June 25, June 30, July 2, July 12, July 13, and July 17, 2014. For each of these visits, Soldan used a debit card to pay for her merchandise. The PII on her debit card was compromised by the Data Breach. Soldan has suffered and will continue to suffer losses and damages as a result of the Data Breach.

13. Plaintiff Rifet Bosnjak is a resident of Missouri. He shopped at the Defendant-owned Shop 'n Save, located at 1253 Water Tower Place in Arnold, Missouri on July 4, 2014.

For this visit, Bosnjak used a debit card to pay for his merchandise. The PII on his debit card was compromised by the Data Breach. Bosnjak has suffered and will continue to suffer losses and damages as a result of the Data Breach.

14. Plaintiff Melissa Alleruzzo is a resident of Missouri. She shopped at the Defendant-owned Shop 'n Save located at 3740 Monticello Plaza in O'Fallon, Missouri on June 25, July 7, and July 14, 2014. For each visit, Alleruzzo used a debit card to pay for her merchandise. The PII on her debit card was compromised by the Data Breach. Alleruzzo has suffered and will continue to suffer losses and damages in the future as a result of the Data Breach.

15. Plaintiff Carol Puckett is a resident of Missouri. She shopped at the Defendant-owned Shop 'n Save located at 2183 Charbonier Road in Florissant, Missouri on June 30 and July 9, 2014. For each visit, Puckett used a debit card to pay for her merchandise. The PII on her debit card was compromised by the Data Breach. Puckett has suffered and will continue to suffer losses and damages in the future as a result of the Data Breach.

16. Defendant is a corporation organized under the laws of Minnesota and has its principal place of business in Minneapolis, Minnesota. Defendant is one of the largest grocery wholesalers and retailers in the U.S., with annual sales of approximately \$17 billion, and around 35,000 employees. Additionally, Defendant provides a wide array of services to its Independent Business retailers, including marketing, merchandising, business, and electronic payment services and infrastructure.

**FACTUAL BACKGROUND**

***The Supervalu Data Breach***

17. At some point prior to or during June 2014, hackers installed malicious software onto Defendant's point-of-sale ("PoS") network—the PoS network includes the cash registers and terminals that handle payment card transactions executed at the Concerned Stores. The malicious software on the PoS network installed by the hackers allowed them to obtain the payment card information of sales transacted at the Concerned Stores.

18. On or about August 14, 2014, Defendant announced in a press release that criminals had gained access to its computer network that processes payment cards transactions for its retail food stores without authorization. *See* Ex. 1. The announcement indicated that 209 Supervalu stores and franchisees, operating as Cub Foods, Farm Fresh, Hornbacher's, Shop 'n Save, and Shoppers Food & Pharmacy, in numerous states, including Minnesota, North Dakota, Illinois, North Carolina, Virginia, Missouri, and Maryland were affected by the Data Breach.

19. The announcement stated that customers who shopped at any of these Supervalu locations between June 22 and July 17, 2014 may have had their names, account numbers, expiration dates, and other numerical information stolen. Thus, for nearly an entire month, unauthorized individuals gained access to Defendant's information systems without Defendant either detecting the malicious software or doing anything to remedy the intrusion.

20. Supervalu customers were not the only ones affected by the Data Breach. Defendant provides information technology and electronic payment services to AB Acquisitions LLC, which operates hundreds of retail stores nationwide under the names Albertsons, ACME Markets, Jewel-Osco, and Shaw's and Star Markets. AB Acquisitions' stores nationwide were affected by the Data Breach, as well.

21. Further, Defendant has announced that “it is possible that time frames, locations and/or at-risk data in addition to those described above will be identified in the future.” Ex. 1. Thus, it is possible that the Data Breach is more expansive in scope than currently believed or admitted.

22. The Data Breach was foreseeable and “completely avoidable.”<sup>1</sup> “These risks are totally avoidable—and at a fraction of the cost of the fallout from dealing with the consequences.”<sup>2</sup> Supervalu failed to meet standards of reasonable conduct and industry best practices designed to prevent attacks like the Data Breach.

23. Defendant’s failure to implement and maintain adequate security measures for the protection of its payment systems, including complying with PCI requirements and standards of reasonable conduct for the protection of its computer systems, provided Defendant with benefits in the form of saving on the costs of compliance, but at the expense and to the detriment of its customers and others harmed—including Plaintiffs and the other Class members here—who have been subjected to the Data Breach or otherwise have had their PII placed at serious and ongoing risk.

24. Defendant allowed the theft of Plaintiffs’ and the other Class members’ PII. Defendant’s conduct did not meet the standards of commercially reasonable steps that should be taken to protect Plaintiffs’ and the other Class members’ PII. Despite being obligated to do so, Defendant failed to employ appropriate technical, administrative, or physical procedures to protect Plaintiffs’ and the other Class members’ PII from unauthorized capture, dissemination, or

---

<sup>1</sup> Tara Seals, Security Researchers: Supervalu PoS Breach “Completely Avoidable” (Aug. 21, 2014), available at <http://www.infosecurity-magazine.com/news/security-researchers-supervalu-pos/> (last visited Aug. 22, 2014).

<sup>2</sup> Eduard Kovacs, Hackers Compromise Point-of-Sale systems at Grocery Giants Supervalu, Albertson’s (Aug. 15, 2014), available at <http://www.securityweek.com/hackers-compromise-point-sale-systems-grocery-giants-supervalu-albertsons> (last visited Aug. 22, 2014).

misuse, thereby making Plaintiffs and the other Class members easy targets for theft and misuse of their financial information, including in the manner undertaken by the hackers here.

***Supervalu Delays Notifying Plaintiffs and the Other Class Members***

25. According to Defendant, approximately one month elapsed between the time the thieves last accessed customers' PII and Defendant disseminated notice of the Data Breach. In that month, Defendant appears to have gained very little information about the Data Breach and deprived Plaintiffs and the other Class Members of an opportunity to take important and effective remedial action to reduce the risk of fraudulent activity in the immediate wake of the Data Breach.

26. Aside from offering to provide only a one-year subscription to credit monitoring services, and rather than take full responsibility for the costs and harm caused by its security failures that resulted in the Data Breach, Defendant has placed the burden on Plaintiffs and the other members of the Class, either to self-monitor their accounts and credit reports for years to come, or to spend time and money replacing accounts and cards, supplemental fraud alerts, and credit-report security freezes.

***Supervalu's Obligation to Protect Customer Information***

27. Defendant accepts customer payments for purchases through credit and debit cards issued by members of the payment card industry ("PCI"), such as Visa, MasterCard, Discover, and American Express. Each of these card issuers has PCI compliance requirements, which are generally similar to one another.<sup>3</sup>

28. In 2006, Visa, MasterCard, and other PCI members established the Security

---

<sup>3</sup> See, e.g., American Express: [www.americanexpress.com/datasecurity](http://www.americanexpress.com/datasecurity); Discover Financial Services: <http://www.discovernetwork.com/merchants/fraud-protection>; MasterCard Worldwide: <http://www.mastercard.com/sdp>; Visa Inc: <http://www.visa.com/cisp> (last visited Aug. 22, 2014).

Standards Council (“PCI SSC”). PCI SSC is an open global forum responsible for the development, management, education, and awareness of PCI Data Security Standards (“PCI DSS”) and related standards for increased security of payment processing systems.

29. Per the PCI SSC, “If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard.”<sup>4</sup>

30. At all times relevant to this action, Defendant was a merchant that accepts payment cards.

31. To adhere to the PCI DSS, a merchant must, *inter alia*:

First, **Assess** -- identify cardholder data, take an inventory of your IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data. Second, **Remediate** -- fix vulnerabilities and do not store cardholder data unless you need it. Third, **Report** -- compile and submit required remediation validation records (if applicable), and submit compliance reports to the acquiring bank and card brands you do business with.

(emphasis in original).<sup>5</sup>

32. PCI compliance also requires that a company “install firewalls and forbid using pass codes that come with applications . . . [and] how credit card data should be stored.”<sup>6</sup>

33. On information and belief, Defendant failed to adequately analyze its computer systems that could expose cardholder data and failed to fix vulnerabilities in its computer systems, which allowed the Data Breach to occur.

---

<sup>4</sup> *How to Be Compliant: Getting Started with PCI Data Security Standard Compliance*, PCI SSC, available at [https://www.pcisecuritystandards.org/merchants/how\\_to\\_be\\_compliant.php](https://www.pcisecuritystandards.org/merchants/how_to_be_compliant.php) (last visited Aug 22, 2014).

<sup>5</sup> *Id.*

<sup>6</sup> Georgina Gustin, *Schnucks Breach Will Likely Cost Millions*, stltoday.com, available at [http://www.stltoday.com/business/local/schnucks-breach-will-likely-cost-millions/article\\_a1cbd2d9-7105-5bfe-8d97-07e2d1381bab.html](http://www.stltoday.com/business/local/schnucks-breach-will-likely-cost-millions/article_a1cbd2d9-7105-5bfe-8d97-07e2d1381bab.html) (last visited Aug. 22, 2014).

34. Further, Defendant is a “Level 1” merchant—in that it processes more than 6 million card transactions a year—which requires it “to undergo quarterly network scans and an annual audit.”<sup>7</sup>

35. In addition,

Under the PCI standards merchants are only allowed to store the data on the front of payment cards—and only if that data is obfuscated. It forbids merchants from storing data found in the magnetic stripes. Information is also required to be encrypted as it travels from point to point in the payment system—from merchant to processor to credit card company to bank—but as [sic] some points it is decrypted as it passes from one to another.<sup>8</sup>

36. Despite these restrictions, Defendant allowed to be compromised the names, account numbers, expirations dates, and other numerical information of Plaintiffs’ and the other Class members’ credit and debit cards in its possession, custody, and control.

***Data Breaches Lead to Identity Theft***

37. The United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”) that identity thieves use personal identifying data to open financial accounts, receive government benefits and incur charges and credit in a person’s name.<sup>9</sup> As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim’s credit rating. In addition, the GAO Report states that victims of identity theft will face “substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name.”

---

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> See Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), available at <http://www.gao.gov/assets/270/262899.pdf> (last visited Aug. 22, 2014).

38. According to the Federal Trade Commission (“FTC”), identity theft wreaks havoc on consumers’ finances, credit history and reputation and can take time, money and patience to resolve.<sup>10</sup> Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.<sup>11</sup>

39. PII—which includes Plaintiffs’ and the other Class members’ customer names combined with their credit or debit card information that were stolen in the Data Breach at issue in this action—is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for a number of years.<sup>12</sup>

40. “The continuation of data breaches at the retail or PoS level is becoming the favored target for hackers and thieves and these breaches are at epidemic proportions,” says Richard Blech, CEO of Proximity.<sup>13</sup>

41. Recent data breaches at Target, Neiman Marcus, Michaels, Sally Beauty, and eBay all underscore the fact that “criminals rather easily leverage existing security weaknesses in corporate networks to gain access to sensitive data and critical PoS systems without being

---

<sup>10</sup> See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at <https://www.cboprf.com/What%20To%20Do%20If%20Your%20Identity%20Is%20Stolen.pdf> (last visited Aug. 22, 2014).

<sup>11</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 CFR § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” *Id.*

<sup>12</sup> Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. See T. Soma, *et al.*, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at \*3–4 (2009).

<sup>13</sup> Tara Seals, *Security Researchers: Supervalu PoS Breach “Completely Avoidable”* (Aug. 21, 2014), available at <http://www.infosecurity-magazine.com/news/security-researchers-supervalu-pos/> (last visited Aug. 22, 2014).

detected.” As a result, “[n]ot making changes to account for this given the ongoing tsunami of headlines about such breaches is equivalent to pure negligence” in the view of some experts.<sup>14</sup>

The fact that these and other high-volume breaches, e.g., the TJX breach, have been occurring for years underscores the care and attention Defendant should have given to the matter.

### ***The Value of Privacy Protections and PII***

42. At a Federal Trade Commission (“FTC”) public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer’s personal information:

The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it’s something on the order of the life blood, the free flow of information.<sup>15</sup>

43. Commissioner Swindle’s 2001 remarks are even more relevant today, as consumers’ personal data functions as a “new form of currency” that supports a \$26 billion per year online advertising industry in the United States.<sup>16</sup>

44. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.<sup>17</sup>

---

<sup>14</sup> *Id.*

<sup>15</sup> Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at [http://www.ftc.gov/sites/default/files/documents/public\\_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf](http://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf) (last visited Aug 22, 2014).

<sup>16</sup> See Julia Angwin and Emily Steel, *Web’s Hot New Commodity: Privacy*, *The Wall Street Journal*, available at <http://online.wsj.com/news/articles/SB10001424052748703529004576160764037920274> (last visited Aug. 22, 2014).

<sup>17</sup> *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), available at <http://www.ftc.gov/sites/default/files/documents/>

45. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from the surrender of their PII.<sup>18</sup> This business has created a new market for the sale and purchase of this valuable data.<sup>19</sup>

46. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that “[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US\$30.49–44.62.”<sup>20</sup>

47. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use—two concerns at issue here—they valued the restriction of improper access to their data at between \$11.33 and \$16.58 per website, and prohibiting secondary use to between \$7.98 and \$11.68 per website.<sup>21</sup>

48. The value of Plaintiffs’ and the other Class members’ PII on the black market is

---

public\_statements /remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited Aug. 22, 2014).

<sup>18</sup> Steve Lohr, *You Want My Personal Data? Reward Me for It*, The New York Times, available at <http://www.nytimes.com/2010/07/18/business/18unboxed.html> (last visited Aug. 22, 2014).

<sup>19</sup> See *Web’s Hot New Commodity: Privacy*, <http://online.wsj.com/news/articles/SB10001424052748703529004576160764037920274>.

<sup>20</sup> Il-Horn Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2002) available <http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (emphasis added) (last visited Aug. 22, 2014); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22 (2) *Information Systems Research* 254, 254 (June 2011).

<sup>21</sup> *Id.*

substantial—credit card numbers range in cost from \$1.50 to \$90 per card number.<sup>22</sup> The New York Times reports that a credit card number alone can fetch as much as \$100.<sup>23</sup> By way of the Data Breach, Defendant has deprived Plaintiffs and the other Class members of the substantial value of their PII, to which they are entitled.

49. Given these facts, any company that transacts business with consumers and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

***Damages Sustained By Plaintiffs and the Other Class Members***

50. A portion of the payments by Plaintiffs and the other Class members necessarily included amounts for Defendant's compliance with industry-standard measures with respect to the collection and safeguarding of PII, including Plaintiffs' and the other Class members' credit and debit card information. Because Plaintiffs and the other Class members were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and the other Class members incurred actual monetary damages in that they overpaid for the products they purchased.

51. Plaintiffs and other members of the Class have suffered and may continue to suffer injury and damages, including, but not limited to: (i) the untimely and inadequate notification of the Data Breach, which has placed Plaintiffs and the other Class members at an increased risk of identity theft and payment card fraud; (ii) improper disclosure of their PII; (iii) loss of and invasion of privacy, and all damages relating thereto that are recoverable at law; (iv) the value of

---

<sup>22</sup> *The Cyber Black Market: What's Your Bank Login Worth*, available at <http://www.ribbit.net/frogtalk/id/50/the-cyber-black-market-whats-your-bank-login-worth> (last visited Aug. 22, 2014); Office of the National Counterintelligence Executive, *How Much Do You Cost on the Black Market*, available at [http://www.ncix.gov/issues/cyber/identity\\_theft.php](http://www.ncix.gov/issues/cyber/identity_theft.php) (last visited Aug. 22, 2014).

<sup>23</sup> Nicole Perlroth, *Supervalu Discloses a Data Breach*, New York Times (Aug. 16, 2014), available at <http://www.nytimes.com/2014/08/16/technology/food-retailer-discloses-a-data-breach.html>. (last visited Aug. 21, 2014).

their time spent mitigating identity theft and payment card fraud and the increased risk of identity theft and payment card fraud; (v) anxiety and emotional distress; and (vi) deprivation of the value of their PII, for which there is a well-established national and international market—for which they are entitled to compensation.

52. Plaintiffs and the other Class members suffered additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend to monitor their financial and bank accounts as a result of the Data Breach. Such damages also include the cost of obtaining replacement credit and debit cards. Defendant is instructing affected customers to take certain steps. Credit and debit card users should review their accounts for unauthorized transactions and notify their banks immediately if they discover any unauthorized purchases or cash advances.

53. Plaintiffs and the other Class members now face a greater risk of identity theft. Debit card users will now be required to take the time to change their PIN numbers on their debit cards, and both credit and debit card users will have to closely review and monitor their accounts for unauthorized activity.

### **CLASS ALLEGATIONS**

54. This action is brought as a class action pursuant to Fed. R. Civ. P. 23, on behalf of a Class defined as follows:

All persons who, between June 22, 2014 and July 17, 2014, authorized a transaction using a payment card at any of the following: a Supervalu store, including any Cub Foods, Farm Fresh, Hornbacher's, Shop 'n Save, and Shoppers Food & Pharmacy; a franchise Cub Foods store; and any Albertsons, ACME Markets, Jewel-Osco, Shaw's, and Star Market (the "Class").

Excluded from the Class are: (i) Supervalu and its officers and directors, (ii) all Class Members who timely and validly request exclusion from the Class, (iii) the Judge presiding over this action, and (iv) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or

abetting the criminal activity occurrence of the Data Breach or who pleads *nolo contendere* to any such charge.

55. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

56. The members of the Class are so numerous that joinder of the Class members would be impracticable. On information and belief, Class members number in the millions. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from Defendant's records.

57. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- a. whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and the other Class members' PII;
- b. whether Defendant properly implemented its purported security measures to protect Plaintiffs' and the other Class members' PII from unauthorized capture, dissemination, and misuse;
- c. whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- d. whether Defendant's delay in informing Plaintiffs and the other Class members of the Data Breach was unreasonable;
- e. whether Defendant's method of informing Plaintiffs and the other Class members of the Data Breach (and its description of the breach and potential exposure to damages as a result of same) was unreasonable;
- f. whether Defendant's conduct violated the Minnesota Deceptive Trade Practices Act, Minn. Stat. § 325D.43, *et. seq.*;
- g. whether Defendant's conduct constitutes breach of an implied contract;
- h. whether Defendant willfully, recklessly or negligently failed to maintain

or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the other Class members' PII;

- i. whether Defendant was negligent in failing to properly secure and protect Plaintiffs' and the other Class members' PII;
- j. whether by publicly disclosing Plaintiffs' and the other Class members' PII without authorization, Defendant invaded Plaintiffs' and the other Class members' privacy; and
- k. whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

58. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

59. Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendant's uniform misconduct described above and were thus all subjected to the Data Breach alleged herein. Further, there are no defenses unique to Plaintiffs that are available to Defendant.

60. Plaintiffs are adequate Class representatives because they will fairly represent the interests of the Class. Plaintiffs have retained counsel with substantial experience in prosecuting consumer class actions, and particularly, data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Class they represent, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse or antagonistic to those of the Class.

61. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs

and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system should not be required to undertake such an unnecessary burden. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## **CAUSES OF ACTION**

### **COUNT I**

#### **Breach of Contract Implied in Fact**

62. Plaintiffs incorporate and reallege paragraphs 1–61, as if fully set forth herein.

63. Customers who made purchases at the Concerned Stores with debit or credit cards were required to provide their card's magnetic stripe data and PINs (for debit cards)—their PII—for payment verification.

64. In providing such PII, Plaintiffs and the other members of the Class entered into an implied contract, whereby Defendant became obligated to reasonably safeguard Plaintiffs' and the other Class members' PII.

65. Under the implied contract, Defendant was obligated not only to safeguard the PII, but also to provide Plaintiffs and the other Class members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

66. Defendant breached the implied contract with Plaintiffs and the other members of the Class by failing to take reasonable measures to safeguard their PII.

67. Defendant also breached its implied contract with Plaintiffs and the other Class members by failing to provide prompt, adequate notice of the Data Breach and unauthorized access of their PII.

68. Plaintiffs and the other Class members have suffered and may continue to suffer injury and damages, including, but not limited to: (i) the untimely and inadequate notification of the Data Breach, which has placed Plaintiffs and the other Class members at an increased risk of identity theft and payment card fraud; (ii) improper disclosure of their PII; (iii) loss of and invasion of privacy, and all damages relating thereto that are recoverable at law; (iv) the value of their time spent mitigating identity theft and payment card fraud and the increased risk of identity theft and payment card fraud; (v) anxiety and emotional distress; and (vi) deprivation of the value of their PII, for which there is a well-established national and international market— for which they are entitled to compensation. At the very least, Plaintiffs and the other Class members are entitled to nominal damages.

## **COUNT II**

### **Violation of Minnesota Deceptive Trade Practices Act, Minn. Stat. § 325D.43, et. seq.**

69. Plaintiffs incorporate and reallege paragraphs 1–61 as if fully set forth herein.

70. Plaintiffs bring this action as a private attorney general acting on their own behalf, pursuant to Minn. Stat. § 325D.43, *et. seq.* and Minn. Stat. § 8.31.

71. Plaintiffs are acting in this capacity to remedy the ongoing unlawful, unfair, and fraudulent business practices alleged herein, and to seek injunctive relief and restitution.

72. The foregoing acts and omissions of the Defendant affect inclusively trade and commerce and affect sponsorship of goods and services in Minnesota.

73. The Minnesota Deceptive Trade Practices Act defines unfair competition to include any unlawful, unfair, or fraudulent business act or practice.

74. Defendant's actions in connection with its failures to adequately protect the PII of Plaintiffs and other members of the Class, and its misconduct regarding the confidential cardholder information constituted deceptive acts and unfair trade practices, having a direct and substantial effect in Minnesota and throughout the United States causing substantial injury to Plaintiffs and the other Class members.

75. Specifically, Defendant violated Minn. Stat. § 325D.44(5) by representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not have" when it represented that it protected Plaintiffs' and the other Class members' PII.

76. Defendant also violated Minn. Stat. § 325D.44(7) by representing that "goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model" but offering goods or services of inferior an standard, quality or grade, when it represented that it protected Plaintiffs' and the other Class members' PII.

77. These violations were a matter of Defendant's standard corporate policy and constitute a consistent pattern and practice of unlawful corporate behavior.

78. Defendants' misrepresentations and failures to make accurate representations were made knowingly or with reason to know that Plaintiffs would rely thereon.

79. Defendant's misrepresentations and failures to make accurate representations were material to Plaintiffs' transactions.

80. Plaintiffs did reasonably and detrimentally rely on Defendant's misrepresentations and failures to make accurate representations. Plaintiffs were damaged thereby and suffered substantial ascertainable losses.

81. Defendant's acts and practices constitute fraudulent business practices in that said acts and practices are likely to deceive the public and affect consumers as to their legal rights and obligations and by use of such deception, falsifying documents, and concealment, may preclude consumers from exercising legal rights to which they are entitled.

**COUNT III**  
**Negligence**

82. Plaintiffs incorporate and reallege paragraphs 1–61 as if fully set forth herein.

83. Defendant owed a duty to Plaintiffs and the other Class members to use and exercise reasonable and due care in safeguarding and protecting the PII of Plaintiffs and the other Class members.

84. Defendant breached its duty to exercise reasonable care in failing to implement reasonable and industry-standard security measures to protect the PII of Plaintiffs and the other Class members.

85. It was foreseeable that Defendant's failure to exercise reasonable care in protecting the PII of Plaintiffs and other Class members would result in Plaintiffs and the other Class members suffering losses and damages.

86. As a direct result of Defendant's failure to secure and protect the PII, Plaintiffs and the other Class members were damaged and may continue to suffer injury and damages, including but not limited to: (i) the untimely and inadequate notification of the Data Breach, which has placed Plaintiffs and the other Class members at an increased risk of identity theft and payment card fraud; (ii) improper disclosure of their PII; (iii) loss of and invasion of privacy, and

all damages relating thereto that are recoverable at law; (iv) the value of their time spent mitigating identity theft and payment card fraud and the increased risk of identity theft and payment card fraud; (v) anxiety and emotional distress; and (vi) deprivation of the value of their PII, for which there is a well-established national and international market—for which they are entitled to compensation.

87. Defendant's wrongful actions and inaction (as described above) constituted negligence at common law.

**COUNT IV**  
**Invasion of Privacy By Public Disclosure of Private Facts**

88. Plaintiffs incorporate and reallege paragraphs 1–61 as if fully set forth herein.

89. Plaintiffs' and the other Class members' PII was (and continues to be) private information.

90. Defendant's failure to secure and protect Plaintiffs' and the other Class members' PII directly resulted in the public disclosure of such private information.

91. Dissemination of Plaintiffs' and the other Class members' PII is not of a legitimate public concern; publicity of their PII would be, is, and will continue to be offensive to Plaintiffs and the other Class members.

92. Plaintiffs and the other Class members were, and continue to be, damaged as a direct and proximate result of Defendant's invasion of their privacy by publicly disclosing their private facts (*i.e.*, their PII) in the form of, *inter alia*: (i) the untimely and inadequate notification of the Data Breach, which has placed Plaintiffs and the other Class members at an increased risk of identity theft and payment card fraud; (ii) improper disclosure of their PII; (iii) loss of and invasion of privacy, and all damages relating thereto that are recoverable at law; (iv) the value of their time spent mitigating identity theft and payment card fraud and the increased risk of

identity theft and payment card fraud; (v) anxiety and emotional distress; and (vi) deprivation of the value of their PII, for which there is a well-established national and international market— for which they are entitled to compensation.

93. Defendant's wrongful actions and inaction (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and the other Class members' privacy by publicly disclosing their private facts (*i.e.*, their PII).

### **REQUEST FOR RELIEF**

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

- A. declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives and appointing Plaintiffs' counsel as Counsel for the Class;
- B. declaring that Defendant breached its implied contract with Plaintiffs and the other Class members;
- C. declaring that Defendant violated the Minnesota Deceptive Trade Practices Act;
- D. declaring that Defendant negligently caused unauthorized access to Plaintiffs' and the other Class members' PII;
- E. declaring that Defendant has invaded Plaintiffs' and the other Class members' privacy;
- F. ordering Defendant to pay actual damages to Plaintiffs and the Class;
- G. ordering Defendant to pay attorneys' fees, litigation costs, and expenses to Plaintiffs and the Class;
- H. ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and
- I. ordering such other and further relief as the Court deems just and proper.

**JURY TRIAL DEMAND**

Plaintiffs, individually and on behalf of all others similarly situated, hereby request a jury trial, pursuant to Federal Rule of Civil Procedure 38, on all claims so triable.

DATED: August 22, 2014

Respectfully submitted,

s/ Rhett A. McSweeney

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

OF COUNSEL:

Ben Barnow  
Erich P. Schork  
Jeffrey Blake  
BARNOW AND ASSOCIATES, P.C.  
1 North LaSalle Street, Suite 4600  
Chicago, Illinois 60602  
(312) 621-2000 (p)  
(312) 641-5504 (f)  
[b.barnow@barnowlaw.com](mailto:b.barnow@barnowlaw.com)  
[e.schork@barnowlaw.com](mailto:e.schork@barnowlaw.com)  
[j.blake@barnowlaw.com](mailto:j.blake@barnowlaw.com)

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

## General Information

|                       |  |
|-----------------------|--|
| <b>Court</b>          | United States District Court for the District of Minnesota; United States District Court for the District of Minnesota |
| <b>Nature of Suit</b> | Contract - Other[190]  |
| <b>Docket Number</b>  | 0:14-cv-03252  |