UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

IN RE: SuperValu, Inc., Customer Data Security Breach Litigation	Case No. 14-md-02586-ADM-TNL
This Document Relates to All Actions	CONSUMER PLAINTIFFS' FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT
	JURY TRIAL DEMANDED

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs ALYSSA ROCKE, STEVE McPEAK, KATHERIN MURRAY, TIMOTHY ROLDAN, DARLA YOUNG, KENNETH HANFF, IVANKA SOLDAN, RIFET BOSNJAK, MELISSA ALLERUZZO, CAROL PUCKETT, GARY MERTZ, MELISSA THOMPKINS, CHRISTOPHER NELSON, HEIDI BELL, JOHN GROSS, and DAVID HOLMES ("Consumer Plaintiffs"), by and through their attorneys, bring this class action on behalf of themselves and all similarly-situated individuals against SUPERVALU, INC ("Supervalu"), AB ACQUISITIONS LLC ("AB Acquisitions"), and NEW ALBERTSON'S, INC. dba JEWEL-OSCO ("Albertsons") (sometimes collectively, the "Defendants").

INTRODUCTION AND NATURE OF ACTION

1. Consumer Plaintiffs bring this class action against Defendants for their 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 their retail stores, including Cub Foods, Farm Fresh, Hornbacher's, Shop'n Save, Shoppers Food & Pharmacy, Albertsons, ACME Markets, Jewel-Osco, Shaw's, and Star Markets.

2. Defendant Supervalu owns and operates regional grocery stores under the brand names Cub Foods, Farm Fresh, Hornbacher's, Shop'n Save, and Shoppers Food & Pharmacy.

3. In addition to controlling the payment processing at its own stores, Defendant Supervalu provides payment processing services for Defendants AB Acquisition and Albertson's

stores, which operate under various brand names including, but not necessarily limited to, Albertsons, ACME Markets, Jewel-Osco, Shaw's, and Star Markets. Thus, while the affected stores were owned by multiple different entities, Defendant Supervalu provided all of the payment processing.

4. On or about August 14, 2014, Defendant Supervalu announced data thieves had gained unauthorized access to Consumer Plaintiffs' and other Class members' PII through the portion of its computer network that processes payment card transactions for its retail stores and the retail stores owned by Defendant AB Acquisitions and Defendant Albertsons. According to the announcement, between June 22, 2014 and July 17, 2014, the payment card data of customers who shopped at 209 Supervalu-owned retail stores and franchisee stores nationwide was disclosed without authorization to the data thieves.

5. On August 14, 2014, the Defendant AB Acquisitions and Defendant Albertsons likewise announced that payment card data of customers who shopped at Albertson's, ACME Markets, Jewel-Osco, Shaw's and Star Markets 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, between June 22, 2014 and July 17, 2014, was compromised by a data breach. In total, the payment card data of customers who shopped at 836 AB Acquisitions-owned stores was affected.

6. Thereafter, on September 29, 2014, Defendants collectively announced a second data breach took place in late August 2014 or early September 2014, when hackers installed different malware in the portion of Supervalu's computer network that processes payment card transactions at some of its Shop 'n Save, Shoppers Food & Pharmacy and Cub Foods owned and franchised stores, including some of its associated stand-alone liquor stores. This second data breach also affected shoppers, including Consumer Plaintiffs and other members of the Class.

7. Defendants claimed the second data breach was unrelated to the first. Consumer Plaintiffs, however, dispute Defendants' position, and allege the first data breach and the second data breach were related and stem from the same fundamental failures of and by Defendants.

Accordingly, any and all data breaches affecting shoppers at the retail stores owned, operated, licensed, franchised, or serviced by Defendants, from June 2014 to the present, will collectively be referred to as the "Data Breach." The affected retail stores will collectively be referred to as the "Affected Stores."

8. Defendants' security failures enabled the hackers to steal Consumer Plaintiffs' and the other Class members' PII from within Defendants' computer systems and put Consumer 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 Defendants, to exploit and injure consumers by selling the PII to third parties and otherwise using the PII for illicit purposes. That ongoing activity now blankets the Consumer Plaintiffs and the other Class members with a known and documented risk.

9. On information and belief, illicit websites are selling the stolen payment card PII "dumps" to international card counterfeiters and fraudsters, and issuing financial institutions are attempting to mitigate their risk. After purchasing Class members' PII, criminals can create counterfeit credit cards by encoding the stolen payment card PII onto any card with a magnetic stripe and can then use the counterfeit cards to make fraudulent purchases. Similarly, criminals can create fake debit cards with the stolen payment card PII, and withdraw cash from the bank accounts of unsuspecting victims through ATMs.

10. The root cause of the Data Breach was Defendants' failure to fix elementary deficiencies in their security systems, abide by industry regulations, and respond to other similar data breaches directed at retailers. In addition, Defendants failed to abide by best practices and industry standards. Had Defendants acted competently, criminals would have been unable to access the PII of Consumer Plaintiffs and the members of the Class.

11. In addition to failing to prevent the Data Breach, Defendants also failed to timely disclose the extent of the Data Breach, failed to individually notify Consumer Plaintiffs and Class members of the Data Breach in a timely manner, and failed to take other reasonable steps to

clearly and conspicuously inform Consumer Plaintiffs and Class members of the nature and extent of the Data Breach. By failing to provide adequate notice, Defendants prevented Consumer Plaintiffs and Class members from protecting themselves from the consequences of the Data Breach.

12. Defendants' wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Consumer Plaintiffs' and Class members' PII constitute violations of state consumer protection laws and state data breach notification laws, negligence, negligence *per se*, breach of implied contract, and unjust enrichment.

13. Accordingly, Consumer Plaintiffs, individually and on behalf of all other members of the Class, assert claims for violations of state consumer protection laws and state data breach notification laws, negligence, negligence *per se*, breach of implied contract, and unjust enrichment, and seek injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief authorized in equity or by law.

JURISDICTION AND VENUE

14. The Court has original jurisdiction pursuant to 28 U.S.C. § 1332. Consumer Plaintiffs are citizens of states different than Defendants. Additionally, the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and is a class action in which there are in excess of 100 class members and many members of the Class are citizens of a state different from Defendant.

15. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(a) and (b) because Defendant Supervalu resides in this District and a substantial part of the events or omissions giving rise to Consumer Plaintiffs' claims occurred in this judicial district.

PARTIES

16. Plaintiff Gary Mertz is a resident of Missouri. On July 7 and 9, 2014, Plaintiff Mertz shopped at Defendant Supervalu's Shop'n Save, located in Dardenne Prairie, Missouri, and swiped his debit card through a Shop'n Save point-of-sale ("POS") card terminal. On information and belief, Plaintiff Mertz's PII, including the full contents of the magnetic strip of his debit card,

was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Mertz spent time determining if his card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Mertz suffered damages in an amount yet to be determined, as such damages are ongoing and include, but are not limited to, time spent monitoring his account information to guard against potential fraud.

17. Plaintiff Alyssa Rocke is resident of Illinois. Plaintiff shopped at the Jewel-Osco supermarket in Highland Park, Illinois, one of the Affected Stores owned and operated by the AB Defendants, on June 22, 2014, June 29, 2014, July 6, 2014, July 13, 2014, August 30, 2014, September 7, 2014, September 14, 2014, and September 21, 2014, and swiped her debit card through the POS card terminal. On information and belief, Plaintiff Rocke's PII, including the full contents of the magnetic strip of her debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Rocke spent time determining if her card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Rocke suffered damages in an amount yet to be determined, as such damages are ongoing and include, but are not limited to, time spent monitoring his account information to guard against potential fraud.

18. Plaintiff Kenneth Hanff is a resident of Missouri. He shopped at the 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 and swiped his debit card through the POS card terminal. On information and belief, Plaintiff Hanff's PII, including the full contents of the magnetic strip of his debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Hanff spent time determining if his card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. After the data breach, Hanff closed his checking account and opened a new one to prevent fraudulent purchases. As a result, Hanff incurred costs and expenses associated with opening the new account. In

addition, Hanff has suffered and will continue to suffer losses and damages as a result of the Data Breach including, but not limited to, time spent monitoring his other accounts and personal information to guard against further potential fraud.

19. Plaintiff Ivanka Soldan is a resident of Missouri. She shopped at the Shop 'n Save located at 1253 Water Tower Place, Arnold, Missouri, on June 25, June 30, July 2, July 12, July 13, and July 17, 2014, and swiped her debit card through the POS card terminal. On information and belief, Plaintiff Soldan's PII, including the full contents of the magnetic strip of her debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Soldan spent time determining if her card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Soldan suffered damages in an amount yet to be determined, as such damages are ongoing and include, but are not limited to, time spent monitoring her account information to guard against potential fraud.

20. Plaintiff Rifet Bosnjak is a resident of Missouri. He shopped at the Shop 'n Save, located at 1253 Water Tower Place, Arnold, Missouri, on July 4, 2014, and swiped his debit card through the POS card terminal. On information and belief, Plaintiff Bosnjak's PII, including the full contents of the magnetic strip of his debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Bosnjak spent time determining if his card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Bosnjak suffered damages in an amount yet to be determined, as such damages are ongoing and include, but are not limited to, time spent monitoring his account information to guard against potential fraud.

21. Plaintiff Melissa Alleruzzo is a resident of Missouri. She shopped at the Shop 'n Save located at 3740 Monticello Plaza, O'Fallon, Missouri, on June 25, July 7, and July 14, 2014, and swiped her debit card through the POS card terminal. On information and belief, Plaintiff Alleruzzo's PII, including the full contents of the magnetic strip of her debit card, was

compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Alleruzzo spent time determining if her card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Alleruzzo suffered damages in an amount yet to be determined, as such damages are ongoing and include, but are not limited to, time spent monitoring her account information to guard against potential fraud.

22. Plaintiff Carol Puckett is a resident of Missouri. She shopped at the Shop 'n Save located at 2183 Charbonier Road , Florissant, Missouri, on June 30 and July 9, 2014, and swiped her debit card through the POS card terminal. On information and belief, Plaintiff Puckett's PII, including the full contents of the magnetic strip of her debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Puckett spent time determining if her card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Puckett suffered damages in an amount yet to be determined as such damages are ongoing and include, but are not limited to, time spent monitoring her account information to guard against potential fraud.

23. Plaintiff Steve McPeak is a resident of Illinois. McPeak shopped at Defendant Supervalu's stores in St. Clair County, Illinois, and swiped his debit card through the POS card terminal. On information and belief, Plaintiff McPeak's PII, including the full contents of the magnetic strip of his debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff McPeak spent time determining if his card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff McPeak suffered damages in an amount yet to be determined, as such damages are ongoing and include, but are not limited to, time spent monitoring his account information to guard against potential fraud.

24. Plaintiff Katherin Murray is a resident of Illinois. Murray shopped at Defendant Supervalu's stores in Woodriver, Illinois, and swiped her debit card through the POS card

terminal. On information and belief, Plaintiff Murray's PII, including the full contents of the magnetic strip of her debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Murray spent time determining if her card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Murray suffered damages in an amount yet to be determined, as such damages are ongoing and include, but are not limited to, time spent monitoring her account information to guard against potential fraud.

25. Plaintiff Timothy Roldan is a resident of Missouri. Roldan shopped at Defendant Supervalu's locations in St. Louis County, Missouri, and swiped his debit card through the POS card terminal. On information and belief, Plaintiff Roldan's PII, including the full contents of the magnetic strip of her debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Roldan spent time determining if his card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Roldan suffered damages in an amount yet to be determined as such damages are ongoing and include, but are not limited to, time spent monitoring his account information to guard against potential fraud.

26. Plaintiff Darla Young is a resident of Missouri. Young shopped at Defendant Supervalu's locations in St. Louis and St. Charles Counties, Missouri, and swiped her debit card through the POS card terminal. On information and belief, Plaintiff Young's PII, including the full contents of the magnetic strip of her debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Young spent time determining if her card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Young suffered damages in an amount yet to be determined as such damages are ongoing and include, but are not limited to, time spent monitoring her account information to guard against potential fraud.

27. Plaintiff Melissa Thompkins is a resident of Maryland. Thompkins shopped at Defendant AB Acquisitions-owned Shopper's Food locations in Ellicott City and Baltimore, Maryland, and swiped her debit card through Defendants' POS card terminal. On information and belief Thompkins' PII was compromised as a result of Defendants' security failures. When the Data Breach was announced, Plaintiff Thompkins spent time determining if her card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise, Thompkins suffered losses and damages in an amount yet to be completely determined, as such losses and damages are ongoing and include, but are not limited to, time spent monitoring her account information to guard against potential fraud.

28. Plaintiff Christopher Nelson is a resident of Pennsylvania. Nelson shopped at Defendant AB Acquisitions-owned ACME Food stores in Avondale, Pennsylvania, and Lantana Square, Delaware, and swiped his credit and debit cards through Defendants' POS terminals. On information and belief Nelson's PII was compromised as a result of Defendants' security failures. When the Data Breach was announced, Plaintiff Nelson spent time determining if his card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise, Nelson suffered losses and damages in an amount yet to be completely determined, as such losses and damages are ongoing and include, but are not limited to, time spent monitoring his account information to guard against potential fraud.

29. Plaintiff Heidi Bell is a resident of Idaho. Bell shopped at Defendant Albertson's stores in Boise, Idaho, and swiped her credit card and debit card through Defendants' POS terminals. On information and belief Bell's PII was compromised as a result of Defendants' security failures. When the Data Breach was announced, Plaintiff Bell spent time determining if her card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise, Bell suffered losses and damages in an amount yet to be completely determined, as such losses and damages are ongoing

and include, but are not limited to, time spent monitoring her account information to guard against potential fraud.

30. Plaintiff John Gross is a resident of New Jersey. Gross shopped at Defendant AB Acquisition's ACME store in Woodbury, New Jersey, on July 11, 2014 and September 17, 2014, and swiped his credit card and debit card through Defendants' POS terminals. On information and belief Gross' PII was compromised as a result of Defendants' security failures. When the data breach was announced, Plaintiff Gross spent time determining if his card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise, Gross suffered losses and damages in an amount yet to be completely determined, as such losses and damages are ongoing and include, but are not limited to, time spent monitoring his account information to guard against potential fraud.

31. Plaintiff David Holmes is a resident of Illinois. Holmes shopped at the Shop 'n Save location in Belleville, Illinois, and swiped his credit card through Defendants' POS terminals. On information and belief Holmes' PII was compromised as a result of Defendants' security failures. When the Data Breach was announced, Plaintiff Holmes spent time determining if his card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. Shortly thereafter, 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 and include, but are not limited to, time spent monitoring his account information to guard against potential fraud.

32. As a direct and/or proximate result of Defendants' wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Consumer Plaintiffs' PII, Consumer Plaintiffs have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) invasion of privacy, (ii) breach of the confidentiality of their PII by Defendants' unauthorized release and disclosure, (iii) lost benefit of their bargain, (iv) deprivation of the value of their PII,

for which there is a well-established national and international market, (v) diminished value of PII protection services purchased from Defendants, (vi) the untimely and inadequate notification of the Data Breach, (vii) the resulting increased risk of future ascertainable losses, economic damages and other actual injury and harm, and (viii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and payment card accounts.

33. Defendant Supervalu Inc. is a Delaware corporation with its headquarters and principal place of business in Eden Prairie, Minnesota. Supervalu is 94th on the 2014 Fortune 500 list and the third-largest food retailing company in the United States. With annual sales of approximately $17 billion and approximately 35,000 employees, Supervalu serves customers across the United States, including Idaho, through a network of 3,320 stores composed of (i) 1,805 independent stores serviced primarily by its food distribution business, (ii) 1,325 Save-A-Lot stores, of which 931 are operated by licensee owners, and (iii) 190 traditional retail grocery stores (store counts as of June 14, 2014)—under the names Cub Foods, Farm Fresh, Hornbacher's, Shop 'n Save, and Shoppers Food & Pharmacy. Under certain contracts with the AB Defendants, Supervalu also provides information technology services to supermarket chains owned by the AB Defendants including, without limitation, Albertson's, ACME Markets, Jewel-Osco, Shaw's and Star Markets—all of which are Affected Stores.

34. Defendant AB Acquisitions, LLC is a privately owned company.[1] Upon information and belief, AB Acquisitions is a Delaware limited liability company with its headquarters and principal place of business in Boise, Idaho. It owns and operates 1,060 supermarkets and 14 distribution centers in 29 states. Through its wholly-owned subsidiary, New Albertson's, Inc., AB Acquisition owns, controls, and operates ACME Markets, Jewel-Osco, Shaw's, and Star Markets—all of which are Affected Stores.

35. Defendant New Albertson's, Inc. is an Ohio corporation. New Albertson's, Inc. is a wholly-owned subsidiary of AB Acquisition, LLC, with its principal operations in Boise, Idaho.

[1] The owners are Cerberus Capital Management, Kimco Realty Corporation, Klaff Realty, Lubert-Adler Partners, and Schottenstein Stores Corporation.

Through New Albertson's, Inc., AB Acquisition, LLC owns, controls, operates, and conducts business as ACME Markets, Jewel-Osco, Shaw's, Star Markets—all of which are Affected Stores.

FACTUAL BACKGROUND

I. The Breach.

36. According to Defendants, from June 22, 2014, to July 17, 2014, hackers accessed and installed malicious software onto Supervalu's unprotected point-of-sale ("POS") network, which includes the cash registers and terminals that process payment card transactions at the Affected Stores. The malicious software released and disclosed the payment card information of sales (*i.e.*, Consumer Plaintiffs' and Class Members' PII) transacted at 209 stores owned, operated and/or franchised by Defendant Supervalu[2] and 836 stores owned operated and/or franchised by Defendant AB Acquisitions.[3]

37. Defendant Supervalu has stated "it is possible that time frames, locations and/or at-risk data in addition to those described above will be identified in the future." *See* Supervalu, Press Release, *available at*, http://www.supervalu.com/security.html. Thus, it is entirely possible that the initial part of the Data Breach is more expansive than currently believed or admitted.

38. Upon information and belief, hackers used remote access tools/points, such as LogMeIn or Microsoft Remote Desktop to gain access to Defendants' networks. Once these access tools/points were identified, hackers were able to gain access to Defendants' networks because Defendants utilized weak passwords and usernames, failed to employ lockout security procedures,[4] and failed to enable multifactor authentication at their remote access points. Upon

[2] Stores affected include Hornbacher's in Minnesota and North Dakota, Cub Foods in Minnesota and Illinois, Farm Fresh in North Carolina and Virgina, Shop'n Save in Illinois and Missouri, and Shoppers in Maryland and Virginia.

[3] Stores affected include Albertsons stores in Southern California, Idaho, Montana, North Dakota, Nevada, Oregon, Washington, Wyoming and Southern Utah, ACME Markets in Pennsylvania, Maryland, Delaware and New Jersey, Jewel-Osco stores in Iowa, Illinois and Indiana, and Shaw's and Star Markets stores in Maine, Massachusetts, Vermont, New Hampshire and Rhode Island.

[4] Lockout security procedures thwart hacker attempts to guess usernames and passwords by locking out IT addresses when multiple failed login attempts occur.

information and belief, Defendants used default passwords or used common, easily guessed passwords, such as passwords based on company name or brand of POS.

39. After gaining access to Defendants' network, hackers gained access to the PII of consumers, including Consumer Plaintiffs and the Class. That access was possible, in large part, because Defendants failed to take adequate measures to protect the PII of Consumer Plaintiffs and the Class.

40. First, because Defendants did not segregate access to their POS terminals from the larger payment network, hackers were able to gain access to a large number of POS terminals by simply gaining access to the larger payment processing network. Moreover, because there were not individual firewalls protecting the POS terminals, hackers were able to install RAM scrapper malware to multiple locations from a single point of access.[5] Following installation, the hackers were then able to harvest consumer information from these multiple locations.

41. Second, hackers also were able to access Consumer Plaintiffs' and Class members' PII that Defendants had improperly stored on their network after customers made purchases at Defendants' stores.

42. Because the hackers were able to access customer records in Defendants' storage, and the actual magnetic strip data with the RAM scrapper malware, they had access to a host of PII including all contents of the magnetic strip found on Consumer Plaintiffs' and other Class members' payment cards.

43. According to Defendants, approximately one month elapsed between the time Consumer Plaintiffs' and Class members' PII was improperly accessed and the time Defendants disseminated notice of the unauthorized PII access to Consumer Plaintiffs and Class members. Defendants' unwarranted delay in notifying Consumer Plaintiffs and Class members about the

[5] RAM scraper malware works as follows: when a card is swiped or entered at a POS terminal the terminal, for a short time, processes the card data unencrypted on its random access memory ("RAM"). Hackers use RAM scraper malware, the type of malware installed on Defendants' POS terminals, to harvest this unencrypted information and thereafter send it to call-home servers. As a result, an attack at the POS means hackers were able to, and did, access all information on the magnetic strip of a payment card, including unencrypted PINs and internal CVV codes. Thus, the theft was not limited to account numbers, expiration dates and names.

unauthorized PII disclosure deprived them of the opportunity to take effective remedial action to reduce the short and long term risk of further fraudulent activity.

44. Thereafter, on September 29, 2014, Defendants announced a second unauthorized PII disclosure took place in late August or early September 2014, when hackers installed different malware in the portion of Supervalu's computer network that processes payment card transactions. This second unauthorized PII disclosure affected shoppers at stores owned and operated by the AB Defendants. Plaintiffs assert that the two unauthorized disclosures were simply two parts of one ongoing and continuous Data Breach.

45. Aside from offering Class Members one-year of credit monitoring services, and rather than taking full responsibility for the ascertainable losses, economic damages and other actual injury and harm caused by the Data Breach, Defendants have placed the burden on Consumer Plaintiffs and Class members to either self-monitor their accounts and credit reports for years to come, or spend time and money replacing accounts and payment cards, placing supplemental fraud alerts, and instituting credit report security freezes.

II. The Breach Was Entirely Avoidable and Foreseeable by Defendants.

46. The initial unauthorized PII disclosure of the Data Breach was foreseeable and "completely avoidable." *See* 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 June 24, 2015); Eduard Kovacs, *Hackers Compromise Point-of-Sale Systems at Grocery Giants Supervalu, Albertson's* (Aug. 15, 2014), available at https://www.securityweek.com/hackers-compromise-point-sale-systems-grocery-giants-supervalu-albertsons (last visited June 24, 2015) ("These risks are totally avoidable—and at a fraction of the cost of the fallout from dealing with the consequences."). And, of course, the second part of the Data Breach, even more so. In fact, Defendants could (and should) have prevented the breach by evaluating their information system architecture, complying

with well-known industry requirements, and heeding the warnings provided by other data breaches directed at retailers like Defendants.

47. First, Defendants should have foreseen the Data Breach and prevented its occurrence because the deficiencies in Defendants' security system that allowed for the RAM scraper malware to be installed on Supervalu's POS terminals, such as lack of 1) lockout controls and two factor authentication, 2) individual firewalls for each POS terminal, and 3) sophisticated usernames and passwords, are elementary security measures that even the most inexperienced IT professional would identify as problematic.

48. These security flaws and other infirmities were explicitly outlined by Visa, as early as 2009, when it issued a Data Security Alert outlining the threat of RAM scraper malware.[6] The report instructs companies to "[s]ecure remote access connectivity," "[i]mplement a secure network configuration, including egress and ingress filtering to only allow the ports/services necessary to conduct business" (i.e., segregate networks), "actively monitor logs of network components, including IDS [intrusion detection systems] and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses," "[e]ncrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit" and "[w]ork with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration."

49. Despite the simplicity of these security flaws and Visa's warning about their existence and potential danger, Defendants failed to take any corrective action and instead neglected their network security and failed to protect Consumer Plaintiffs and the Class.

50. Second, Defendants' security flaws ran afoul of best practices and industry standards. If Defendants would have followed these practices and complied with industry

[6] The Visa report can be found here: https://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf (last visited June 24, 2015).

standards the Breach would not have occurred.

51. All merchants that accept customer payments via payment cards, including Defendants, are obligated and required to comply with the Payment Card Industry Data Security Standards (the "PCI DSS"). *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 (last visited June 24, 2015) (stating "[i]f you are a merchant that accepts payment cards, you are required to be complaint with the PCI [DSS]."). Compliance with the PCI DSS is common practice in the retail industry.

52. The PCI DSS, among other things, mandates merchants to protect cardholder data, PCI DSS v. 3.0 at 34 (Nov. 2013),[7] requires merchants to install and maintain firewalls, *id.* at 19, forbids merchants from using default settings and passwords for applications and devices, *id.* at 28, requires merchants to segment cardholder data, *id.* at 61, and requires merchants to identify and authenticate their system users. *Id.* at 64.

53. Additionally, sub-requirement 3.2 of the PCI DSS requires merchants and other organizations involved in payment card transactions to refrain from storing sensitive authentication data after authorization (even if it is encrypted). *See id.* at 35.

54. 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.

[7] A copy of PCI DSS v. 3.0 can be found at: https://www.pcisecuritystandards.org/security_standards/documents.php?agreements=pcidss&association=pcidss (last visited June 24, 2015).

(emphasis in original). *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 (last visited June 24, 2015).

55. As a "Level 1" merchant, Supervalu was further required "to undergo quarterly network scans and an annual audit." 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 (last visited June 24, 2015).

56. Furthermore, storing information from the magnetic stripe of consumer credit/debit cards is strictly prohibited.

> 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.

Id.

57. Despite these well-documented and well-known industry restrictions and mandates, Defendants failed to properly secure their systems to protect cardholder data. Indeed, the security practices (or lack thereof) instituted by Defendants directly conflict with the PCI DSS core security standards, including standards 1-3 and 7-8. Had Defendants taken their obligations seriously, the breach would not have occurred.

58. Third, Defendants were on notice of the very real possibility of consumer data theft associated with their security practices. Security flaws similar to the ones exploited in the Breach have previously exposed sensitive consumer information to hackers in recent retail data breaches, such as the Target breach and the Neiman Marcus and Michaels Stores breaches. In addition, on August 1, 2007, the Minnesota Legislature passed the Minnesota Plastic Card Security Act ("PCSA"), which sets strict time limitations on the retention of credit and debit card information by retailers. *See* Minn. Stat. § 325E.64. This legislation, along with the PCI DSS alerted

Defendants to the risks associated with storage of consumer data. Defendants disregarded those risks and chose to store their customers' sensitive data.

59. Despite the fact that Defendants were on notice of the very real possibility of consumer data theft associated with their security practices and despite the fact that Defendants knew or, at the very least, should have known, about the elementary infirmities associated with their security systems, they still failed to make any changes to their security practices and protocols. Consequently, hackers were able to access Consumer Plaintiffs' and Class members' PII with ease.

60. As a result of Defendants' indifference to the sensitive nature of Consumer Plaintiffs' PII, both in Defendants' failure to employ adequate security measures and Defendants' failure to delete promptly its customers' sensitive data, Consumer Plaintiffs' PII, as well as the PII of Class members, has been exposed to criminals. This exposure has made the financial accounts of Consumer Plaintiffs and the members of the Class less secure and has subjected them to an imminent and real possibility of identity theft.[8]

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. Despite being obligated to do so, Defendants failed to employ appropriate technical, administrative, or physical procedures to protect the PII of Consumer Plaintiffs and the Class from unauthorized capture, dissemination, or misuse, thereby making Consumer 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.

[8] Indeed, stolen information is often used well after the data breach in question. Recently, thieves attempted to charge thousands of dollars to a credit card that was compromised in the Home Depot data breach more than a year prior. *See* Stephen Montemayor, "Eagan woman, Chicago man accused of using stolen credit card numbers", *available at* http://www.startribune.com/eagan-woman-chicago-accused-of-using-credit-card-numbers-compromised-in-home-depot-data-breach/308201391/ (last visited June 24, 2015).

III. The Personal Information and Privacy of Consumers is Valuable.

62. The PII of Consumer Plaintiffs and the Class is a valuable property right. *See, e.g.*, John 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) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted). In fact, PII—including Consumer Plaintiffs' names combined with the payment card information disclosed and compromised in the Data Breach—is so valuable to fraudsters that they often buy and sell the information on the well-established national and international "cyber black-market" for years.

63. At a Federal Trade Commission ("FTC") public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's PII:

> 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.

FTC Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, *available at* https://www.ftc.gov/sites/default/files/documents/public _events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited June 24, 2015). 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. *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (online) *available at* http://www.wsj.com/articles/SB10001424052748703529004576160764037920274 (last visited June 24, 2015).

64. 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.

Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/privacyroundtable_dec2009_transcript.pdf (last visited June 24, 2015).

65. Recognizing the high value 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 they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated. 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 June 24, 2015).

66. This business has created a new market for the sale and purchase of this valuable data. *See Web's Hot New Commodity: Privacy*, *available at* http://online.wsj.com/news/articles/SB10001424052748703529004576160764037920274 (last visited June 24, 2015).

67. Consumers place a high value on their PII, as well as on the *privacy* of their PII. Research shows 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." Il-Horn Hann *et al.*, *The Value of Online Information Privacy* (Oct. 2002) *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited June 24, 2015); *see also* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22 (2) Information Systems Research 254, 254 (June 2011).

68. When consumers were surveyed about how much value they place on protecting their PII against improper access and unauthorized secondary use—two concerns at issue here—

they valued the restriction of improper access at between $11.33 and $16.58 per website, and valued the prohibition of secondary use at between $7.98 and $11.68 per website. *Id.*

69. The value of the PII of Consumer Plaintiffs and the Class on the cyber black market is substantial—credit card numbers alone range in cost from $1.50 to nearly $100 per card number. *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 June 24, 2015); National Counterintelligence and Security Center, *How Much Do You Cost on the Black Market*, *available at* http://www.ncix.gov/issues/cyber/identity_theft.php (last visited June 24, 2015).

70. By virtue of the Data Breach and unauthorized release and disclosure of the PII of Consumer Plaintiffs and the Class, Defendants have deprived Consumer Plaintiffs and the Class of the substantial values of their PII, to which they are entitled.

IV. Data Breaches Lead to Identity Theft and Cognizable Injuries.

71. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

72. For example, The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name. *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 June 24, 2015). The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name." *Id.*

73. According to the Federal Trade Commission ("FTC"), unauthorized PII disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), *available at* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited June 24, 2015). Criminals use compromised PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

74. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

75. Indeed, the information identity thieves obtain from breaching corporate networks is so valuable that identify thieves often trade the information on the cyber black market for a number of years after the initial theft.

76. As a result, victims suffer immediate and long lasting exposure and are susceptible to further injury over the passage of time.

77. Most high profile data breaches, including those associated with the TJX Companies and Target, imminently and inevitably lead to identity theft and adverse use of PII, and the very real possibility of theft and adverse use continues into the future, long after the initial breach.

78. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

79. "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. 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 June 24, 2015).

80. Recent data breaches at Home Depot, Target, Neiman Marcus, Michaels, Sally Beauty, and eBay all underscore the fact that "criminals can rather easily leverage existing security weaknesses in corporate networks to gain access to sensitive data and critical PoS systems without being detected." *Id*. 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. *Id*.

81. The fact that these and other high-volume data breaches have been occurring for years underscores the care and attention Defendants should have given to the matter—but, unfortunately did not.

V. Consumer Plaintiffs' and Class Members' Have Suffered Ascertainable Losses, Economic Damages and Other Actual Injury and Harm.

82. As a direct and proximate result of Defendants' wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Consumer Plaintiffs' and other Class Members' PII, Consumer Plaintiffs and the other Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) diminished value of their PII, (ii) the untimely and inadequate notification of the Data Breach, (iii) the resulting increased risk of future ascertainable losses, economic damages and other actual injury and harm, and (iv) the opportunity cost and value of lost time they must spend to monitor their financial accounts and payment card accounts—for which they are entitled to compensation.

CLASS DEFINITION AND ALLEGATIONS

83. Consumer Plaintiffs bring their claims for violations of state consumer protection laws and state data breach notification statutes and unjust enrichment on behalf of themselves and

all other similarly situated persons pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following multi-state classes:

Multi-State [Consumer Protection Law, Data Breach Notification Statute or Unjust Enrichment] Classes:

> All persons who, within the applicable statute of limitations under their respective state's [consumer protection law(s),[9] data breach notification statute,[10] or unjust enrichment law[11]], had their credit or debit card information and/or other personal information compromised as a result of the Data Breach that occurred at Defendants' affected stores between June 22, 2014, and July 17, 2014, and August-September 2014.
>
> Excluded from the Class are: (i) Defendants and their officers, directors, affiliates, parents, and subsidiaries (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 Breaches or who pleads *nolo contendere* to any such charge.

---

[9] The Consumer Protection Laws of the following states are substantially similar: Arkansas (Ark. Code § 4-88-101, *et seq.*); Colorado (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut (Conn. Gen. Stat. § 42-110, *et seq.*); Delaware (Del. Code tit. 6, § 2511, *et seq.*); District of Columbia (D.C. Code § 28-3901, *et seq.*); Florida (Fla. Stat. § 501.201, *et seq.*); Hawaii (Haw. Rev. Stat. § 480-1, *et seq.*); Idaho (Idaho Code § 48-601, *et seq.*); Illinois (815 ICLS § 505/1, *et seq.*); Maine (Me. Rev. Stat. tit. 5 § 205-A, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws § 445.901, *et seq.*); Minnesota (Minn. Stat. § 325F.67, *et seq.*); Missouri (Mo. Rev. Stat. § 407.010, *et seq.*); Montana (Mo. Code. § 30-14-101, *et seq.*); Nebraska (Neb. Rev. Stat. § 59-1601, *et seq.*); Nevada (Nev. Rev. Stat. § 598.0915, *et seq,*); New Hampshire (N.H. Rev. Stat. § 358-A:1, *et seq.*); New Jersey (N.J. Stat. § 56:8-1, *et seq.*); New Mexico (N.M. Stat. § 57-12-1, *et seq.*); New York (N.Y. Gen. Bus. Law § 349,*et seq.*); North Dakota (N.D. Cent. Code § 51-15-01, *et seq.*); Oklahoma (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon (Or. Rev. Stat. § 646.605, *et seq.*); Rhode Island (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Dakota (S.D. Code Laws § 37-24-1, *et seq.*); Texas (Tex. Bus. & Com. Code § 17.41, *et seq.*); Virginia (VA Code § 59.1-196, *et seq.*); Vermont (Vt. Stat. tit. 9, § 2451, *et seq.*); Washington (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia (W. Va. Code § 46A-6-101, *et seq.*); and Wisconsin (Wis. Stat. § 100.18, *et seq.*).

[10] The Data Breach Notification Statutes of the following states are substantially similar: Cal. Civ. Code. § 1798.82 (most expedient time possible and without unreasonably delay); 6 Del. Code Ann. § 12B-102(a) (most expedient time possible and without unreasonable delay); 815 Ill. Comp. Stat. § 530/10(a) (most expedient time possible and without unreasonable delay); Md. Code Ann., Com. Law § 14-3504(b)(3) (as soon as reasonably possible); and Minn. Stat. Ann. § 325E.61(1)(a) (most expedient time possible and without unreasonable delay).

[11] The unjust enrichment laws of the fifty states are consistent across jurisdictions. *See In re Target Corp. Data Sec. Breach Litig.*, MDL 14-md-2522, 2014 WL 7192478, at *22 (D. Minn. Dec. 18, 2014).

84. In the alternative Consumer Plaintiffs bring their claims for violations of state consumer protection laws and state data breach notification statutes and unjust enrichment on behalf of themselves and all other similarly situated persons pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following statewide classes:

> **Statewide [Consumer Protection Law, Data Breach Notification Statute or Unjust Enrichment] Classes:**
>
> All residents of [name of State] whose credit or debit card information and/or other personal information was compromised as a result of the Data Breach that occurred at Defendants' affected stores between June 22, 2014, and July 17, 2014, and August-September 2014.
>
> Excluded from the Class are: (i) Defendants and their officers, directors, affiliates, parents, and subsidiaries (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 Breaches or who pleads *nolo contendere* to any such charge.

85. Consumer Plaintiffs bring their claims for negligence, negligence per se, breach of implied contract and unjust enrichment on behalf of themselves and all other similarly situated persons pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following statewide classes:

> **Statewide [Negligence, Negligence Per Se and Breach of Implied Contract] Class:**
>
> All residents of [name of State] whose credit or debit card information and/or other personal information was compromised as a result of the Data Breach that occurred at Defendants' affected stores between June 22, 2014, and July 17, 2014, and August – September 2014.
>
> Excluded from the Class are: (i) Defendants and their officers, directors, affiliates, parents, and subsidiaries (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 Breaches or who pleads *nolo contendere* to any such charge.

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

87. The members of the Classes are so numerous that joinder of all members of the Classes is impracticable. Consumer Plaintiffs are informed and believe that the proposed Classes contain thousands of purchasers who used payment cards to complete purchases at Defendants' stores who have been damaged by Defendants' conduct as alleged herein. The precise number of Class members is unknown to Plaintiff, but may be ascertained from Defendants' records.

88. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

(1) whether Defendants engaged in the wrongful conduct alleged herein;

(2) whether the alleged conduct constitutes violations of the laws asserted;

(3) whether Defendants owed Consumer Plaintiffs and the other Class members a duty to adequately protect their personal and financial data;

(4) whether Defendants breached their duty to protect the personal and financial data of Consumer Plaintiffs and the other Class members;

(5) whether Defendants knew or should have known about the inadequacies of their payment processing network and the dangers associated with storing sensitive cardholder information;

(6) whether Defendants failed to use reasonable care and commercially reasonable methods to safeguard and protect Consumer Plaintiffs' and the other Class members' PII from unauthorized release and disclosure;

(7) whether the proper data security measures, policies, procedures and protocols were in place and operational within Supervalu's computer systems to safeguard and protect Consumer Plaintiffs'

and the other Class members' PII from unauthorized release and disclosure;

(8) whether Defendants' conduct was the proximate cause of Consumer Plaintiffs' and the other Class members' injuries;

(9) whether Defendants took reasonable measures to determine the extent of the Data Breach after it was discovered;

(10) whether Defendants' delay in informing Consumer Plaintiffs and the other Class members of the Data Breach was unreasonable;

(11) whether Defendants' method of informing Consumer Plaintiffs and the other Class members of the Data Breach was unreasonable;

(12) whether Consumer Plaintiffs and the other Class members suffered ascertainable and cognizable injuries as a result of Defendants' conduct;

(13) whether Defendants' conduct was deceptive, unfair, or unconscionable, or constituted unfair competition;

(14) whether Defendants' conduct was likely to deceive a reasonable consumer;

(15) whether Consumer Plaintiffs and the other Class members are entitled to recover actual damages and/or statutory damages; and

(16) whether Consumer Plaintiffs and the other Class members are entitled to other appropriate remedies, including corrective advertising and injunctive relief.

89. Defendants engaged in a common course of conduct giving rise to the claims asserted by Consumer 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.

90. Consumer Plaintiffs' claims are typical of the claims of the members of the Classes because, inter alia, all Class members were injured through the uniform misconduct described above. Consumer Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all members of the Classes.

91. Consumer Plaintiffs will fairly and adequately protect the interests of the members of the Classes, have retained counsel experienced in complex consumer class action litigation, and

intend to prosecute this action vigorously. Consumer Plaintiffs have no adverse or antagonistic interests to those of the Classes.

92. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

93. Consumer Plaintiffs seek preliminary and permanent injunctive and equitable relief on behalf of the Classes, preventing Defendants from further engaging in the acts described and requiring Defendants to provide full restitution to Consumer Plaintiffs and the other Class members.

94. Unless the Classes are certified, Defendants will retain monies received as a result of their conduct that were taken from Consumer Plaintiffs and the other Class members. Unless Class-wide injunctions are issued, Defendants will continue to commit the violations alleged, and the members of the Classes and the general public will continue to be deceived and injured.

95. Defendants have acted and refused to act on grounds generally applicable to the Classes, making appropriate final injunctive relief with respect to the Classes as a whole.

FIRST CAUSE OF ACTION
(State Consumer Protection Laws)

96. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

97. Consumer Plaintiffs and members of the Multi-State Consumer Protection Law Class, or in the alternative the statewide Consumer Protection Law Class (the "Class" as used in

this count), are consumers who used their credit and/or debit cards to purchase products from Defendants, primarily for personal, family or household purposes.

98. Defendants engaged in the conduct alleged above in transactions intended to result, and which did result, in the sale of goods and services to consumers, including Consumer Plaintiffs and the Class.

99. This course of conduct also affects trade and commerce, nationally and in Minnesota. Defendants' actions and/or inactions regarding their failure to adequately protect the PII of Consumer Plaintiffs and the Class constitute deceptive acts and unfair practices and have a direct and substantial affect in Minnesota and throughout the United States.

100. Defendants' conduct as alleged herein, including without limitation, Defendants' failure to maintain reasonable and adequate computer systems and data security practices, Defendants' fraudulent and deceptive omissions and/or misrepresentations 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 in violation of the following state consumer protection laws:

a. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*, and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq.*;

b. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;

a. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Stat. § 510/2(a)(5), (7) and (12), *et seq.*;

b. The Maryland Consumer Protection Act, Md. Code Com. Law, § 13-301(1) and (2)(i) and (iv) and (9(i), *et seq.*;

c. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), *et seq.*, the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a).

d. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq*;

e. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

f. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq*.

101. Defendants' conduct has violated the state consumer protection laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another, and/or "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;" and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

102. As a result, Defendants' conduct damaged Consumer Plaintiffs and the other members of the Class, who would not have otherwise completed credit and/or debit card purchases/transactions at Defendants' stores, by exposing their information to third-party hackers.

103. Consumer Plaintiffs bring this action on behalf of themselves and all similarly situated persons for the requested relief and for the public benefit at large in order to promote truthful, honest and non-deceptive business practices, which will allow consumers to make informed purchasing decisions and to protect, Consumer Plaintiffs, members of the Class and the public from Defendants' unfair, deceptive, fraudulent, unconscionable and/or unlawful practices and methods of competition. Defendants' conduct as alleged herein has had widespread negative consequences and has affected consumers throughout the nation.

SECOND CAUSE OF ACTION
(State Data Breach Notification Statutes)

104. Consumer Plaintiffs incorporate by reference and reasserts all previous paragraphs.

105. The Data Breach constitutes a breach of Defendants' computer security systems within the meaning of the state data breach notifications statutes listed below, and the data accessed in the Data Breach was protected and covered by the below listed statutes.

106. The names, account numbers, expiration dates, PINs, and other numerical information of the Consumer Plaintiffs and the Class constitute personal information as defined by the state data breach notification statutes listed below.

107. Defendants unreasonably delayed notification of the Data Breach, including the unauthorized access and theft of the PII of their customers, including Consumer Plaintiffs and the Multi-State Data Breach Notification Statute Class, or in the alternative the statewide Data Breach Notification Class (the "Class" as used in this count), after Defendants knew or should have know that the Data Breach had occurred.

108. When the Data Breach began on or about June 22, 2014, Defendants did not disclose or notify the public of the data breach. Defendants knew or should have known that the Data Breach was occurring as early as June 22, 2014, but failed to disclose its existence to the public, including Consumer Plaintiffs and the Class, at this time.

109. From June 22, 2014, until around July 17, 2014, for a period of about a month, Defendants took no action to remedy the Data Breach, or ensure that their systems were properly protecting the PII of Consumer Plaintiffs and the Class. Defendants failed to inform the public of the Data Breach during this time even though Defendants knew or should have known of the Data Breach's occurrence and the attendant unauthorized access, theft and dissemination of Consumer Plaintiffs' and the other Class members' PII.

110. On or around July 17, 2014, when Supervalu finally reacted to the Data Breach and began purging its systems of the malicious hacker software and fixing the unreasonable security holes that led to the Data Breach, Defendants still failed to disclose or provide notice to the public that the Data Breach had occurred.

111. Defendants waited until August 14, 2014, almost a month after they purged their computer systems and remedied their security deficiencies and almost two months after the Breach began, to disclose the Data Breach and notify their customers. In their initial disclosure and in their September 29, 2014, update on the Data Breach, Defendants downplayed the significance of the Data Breach and claimed that they did not know whether Personal Information was stolen and that there was no evidence of misuse of any customer Personal Information.

112. Furthermore, Defendants claimed that the Data Breach was under control in their initial August 14, 2014 disclosure, but on September 29, 2014, alerted customers to a second breach.

113. Defendants failed to disclose to Consumer Plaintiffs and the other Class members, without unreasonable delay and in the most expedient time possible, the Data Breach and the unauthorized access and theft of the PII of Consumer Plaintiffs and the other Class members when Defendants knew, should have known, or reasonably believed that such information had been compromised. In addition, Defendants' claimed the Data Breach was under control on August 14, 2014, but disclosed on September 29, 2014, that the Data Breach was still ongoing.

114. On information and belief, no law enforcement agency instructed Defendants to withhold notification and disclosure of the Data Breach.

115. As a result of Defendants' failure to notify in the statutorily prescribed time periods, Consumer Plaintiffs and the other Class members suffered the direct harm as alleged above.

116. Had Defendants provided timely and accurate notice, Consumer Plaintiffs and members of the Class could have taken steps to mitigate the direct harm suffered as a result of Defendant's unreasonable and untimely delay in providing notice. Consumer Plaintiffs and the other members of the Class could have used cash instead of credit and debit cards in closing sales transactions at Defendants' stores, avoided shopping at the stores altogether, contacted their financial institutions to cancel cards and accounts, or taken other steps in efforts to avoid the direct harm caused by Defendants' failure to notify. Furthermore, had Defendants truthfully disclosed

the Breach and the lack of security surrounding their systems on August 14, 2014, Consumer Plaintiffs and the other Class members could have refrained from shopping at Defendants' stores and being subjected to subsequent unauthorized access that occurred between August 14, 2014, and September 29, 2014, the date Defendants disclosed that their systems still were not adequately protected.

117. Defendants' failure to notify Consumer Plaintiffs and the other Class members violated the following state data breach notification statutes:

a. Idaho Code Ann. § 28-51-105(1), *et seq.*;

b. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

c. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

d. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

e. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*; and

f. N.J. Stat. Ann. § 56:8-163(a), et seq.

118. Consumer Plaintiffs and the other members of the Class seek all remedies available under the applicable state data breach notification statutes, including but not limited to damages as alleged above, equitable relief and reasonable attorneys' fees, and costs, as provided by law.

THIRD CAUSE OF ACTION
(Negligence)

119. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

120. A special relationship exists between Defendants and the Consumer Plaintiffs and the statewide Negligence Class (the "Class" as used in this count). Defendants actively solicited Consumer Plaintiffs and the other Class members to use their PII in sales transactions at Defendants' stores. When Consumer Plaintiffs and the other Class members gave their PII to Defendants to facilitate and close sales transactions, they did so with the mutual understanding that Defendants had reasonable security measures in place and Defendants would take reasonable steps to protect and safeguard the PII of Consumer Plaintiffs and the other Class members. Consumer Plaintiffs and the other Class members also gave their PII to Defendants on the premise

that Defendants were in a superior position to protect against the harms attendant to unauthorized access, theft and misuse of that information.

121. Upon gaining access to the PII of Consumer Plaintiffs and members of the Class, Defendants owed to Consumer Plaintiffs and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed and misused by unauthorized parties. Pursuant to this duty, Defendants were required to design, maintain and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PII of Consumer Plaintiffs and the Class. Defendants further owed to Consumer Plaintiffs and the Class a duty to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

122. Defendants owed this duty to Consumer Plaintiffs and the other Class members because Consumer Plaintiffs and the other Class members compose a well-defined, foreseeable and probable class of individuals whom Defendants should have been aware could be injured by Defendants' inadequate security protocols. Defendants actively solicited Consumer Plaintiffs and the other Class members to use their PII in sales transactions at Defendants' stores. To facilitate and close these sales transactions, Defendants used, handled, gathered and stored the PII of Consumer Plaintiffs and the other Class members. Attendant to Defendants' solicitation, use and storage, Defendants knew of their inadequate and unreasonable security practices with regard to their computer systems and also knew that hackers routinely attempt to access, steal and misuse the PII that Defendants actively solicited, used and stored from Consumer Plaintiffs and the other Class members. As such, Defendants knew a breach of their systems would cause damage to their customers, including Consumer Plaintiffs and the other Class members. Thus, Defendants had a duty to act reasonably in protecting the sensitive information of their consumers.

123. Defendants also owed this duty to Consumer Plaintiffs and the other Class members because Consumer Plaintiffs and members of the Class entrusted Defendants with their PII by making purchases with their credit and debit cards at Defendants' stores. Defendants knew,

or should have known, of the risk inherent in obtaining, using, handling and storing the PII of Consumer Plaintiffs and the other Class members and of the critical importance in providing adequate security systems to protect such information while it is being gathered, used and stored.

124. Defendants also owed a duty to timely and accurately disclose to Consumer Plaintiffs and the other Class members the scope, nature and occurrence of the Breach. This duty was required and necessary in order for Consumer Plaintiffs and the other Class members to take appropriate measures to avoid unauthorized charges to their credit-and/or debit-card accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring services and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Defendants' unreasonable misconduct.

125. Defendants breached their duties to Consumer Plaintiffs and the other Class members by failing to implement and maintain security systems and controls that were capable of adequately protecting the PII of Consumer Plaintiffs and the other Class members. More specifically, Defendants breached their duties to Consumer Plaintiffs and the other Class members by failing to remedy the deficiencies found in the remote access points to their servers and corporate networks and by storing Consumer Plaintiffs' and the other Class members' data on their servers.

126. Defendants further breached their duties to Consumer Plaintiffs and the other Class members when they failed to fix the deficiencies associated with their security and storage policies despite the fact that they knew or, at the very least, should have known, that these deficiencies were the leading cause of data breaches and theft of sensitive consumer information.

127. Defendants also breached their duties to timely and accurately disclose to the Consumer Plaintiffs and the other Class members that their PII had been or was reasonably believed to have been improperly accessed or stolen.

128. Defendants' negligence in failing to exercise reasonable care in protecting the PII of Consumer Plaintiffs and the other Class members is further evidenced by Defendants' failures

to comply with legal obligations and industry standards, such as the PCI DSS, and the delay between the start of the Data Breach and the time when the Data Breach was disclosed.

129. Defendants' retention of Consumer Plaintiffs and the other Class members' PII on Defendants' servers beyond legal limits, including those imposed by Minn. Stat. § 325E.64, contributed to and facilitated the Data Breach and further evidences Defendants' failure to employ reasonable care in protecting the PII of Consumer Plaintiffs and the Class.

130. The injuries to Consumer Plaintiffs and the other Class members were reasonably foreseeable to Defendants because laws and statutes, such as Minn. Stat. § 325E.64, and industry standards, such as the PCI DSS, require Defendants to safeguard and protect their computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Consumer Plaintiffs' and the other Class members' PII.

131. The injuries to Consumer Plaintiffs and the other Class members also were reasonably foreseeable because Defendants knew or should have known that their computer systems used for processing consumer sales transactions were inadequate and unable to protect solicited consumer PII from being breached, accessed and stolen by hackers and unauthorized third parties. As such, Defendants' own misconduct created a foreseeable risk of harm to Consumer Plaintiffs and the other Class members.

132. Defendants' failure to take reasonable steps to protect the PII of Consumer Plaintiffs and the other members of the Class was a proximate cause of their injuries because it directly allowed hackers easy access to Consumer Plaintiffs' and the other Class members' PII. This ease of access allowed hackers to implement unsophisticated attacks and thereafter steal PII of Consumer Plaintiffs and the other members of the Class and disseminate it over black markets.

133. As a direct proximate result of Defendants' conduct, Consumer Plaintiffs and the other Class members have suffered theft of their PII. Defendants allowed cybercriminals access to Class members' PII, thereby decreasing the security of Class members' bank accounts, making Class members' identities less secure and reliable, and subjecting Class members to the imminent threat of identity theft. Not only will Consumer Plaintiffs and the other members of the Class

have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against the specter of identity theft for years to come.

134. Defendants' conduct warrants moral blame because Defendants actively solicited, used, handled and stored the PII of Consumer Plaintiffs and the other Class members without disclosing that their computer systems used for consumer transactions were inadequate and unable to protect the PII of Consumer Plaintiffs and the other Class members.

135. Holding Defendants accountable under negligence law will further the policies embodied in such law by incentivizing larger retail and grocery store chains to properly secure sensitive consumer information and thereby protect the consumers who rely on these companies every day.

FOURTH CAUSE OF ACTION
(Breach of Implied Contract)

136. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

137. Defendants actively solicited the PII of Consumer Plaintiffs and members of the statewide Breach of Implied Contract Class (the "Class" as used in this count) by offering Consumer Plaintiffs and the other Class members the option of purchasing products at Defendants' stores through use of credit and/or debit cards. Consumer Plaintiffs and the other members of the Class accepted Defendants' offers and used their credit and/or debit cards to purchase products at Defendants' stores.

138. Each purchase that involved use of a credit or debit card was made pursuant to mutually agreed upon implied contract terms that Defendants would take reasonable measures to protect the PII of Consumer Plaintiffs and the other Class members and that Defendants would timely and accurately notify Consumer Plaintiffs and the other Class members if and when such information was compromised.

139. Had such implied contractual terms failed to exist, Consumer Plaintiffs and the other Class members never would have used their credit and debit cards to make purchases at Defendants' stores and never would have entrusted their PII to Defendants for use.

140. Consumer Plaintiffs and the other Class members fully performed their obligations under the implied contractual terms.

141. In contrast, Defendants breached the implied terms of the contracts they made with Consumer Plaintiffs and the other Class members by failing to reasonably protect their PII and by failing to provide adequate notice of the Data Breach and unauthorized access of such information.

142. The damages described herein and suffered by Consumer Plaintiffs and the other Class members were the direct proximate result of Defendant's breach of the implied contractual terms.

FIFTH CAUSE OF ACTION
(Negligence Per Se)

143. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

144. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits "unfair . . . practices in or affecting commerce" including, as recently interpreted by the FTC, the act or practice by retailers, such as Defendants, of failing to take reasonable measures to protect their customers' PII.

145. Defendants violated Section 5 and similar state statues by failing to employ reasonable security systems, controls and procedures to protect the PII of Consumer Plaintiffs and the other Class members. This violation constitutes negligence *per se*.

146. The Consumer Plaintiffs and the statewide Negligence *Per Se* Class are the individuals the FTC Act seeks to protect. For instance, the FTC Act expressly prohibits "unfair" acts that "cause or are likely to cause substantial injury to ***consumers*** which is not reasonably avoidable by ***consumers***."

147. Additionally, the harm that has occurred to Consumer Plaintiffs and the other Class members is the type of harm the FTC Act was intended to prevent and remedy. To be sure, the FTC has pursued a number of enforcement actions against businesses that caused the unauthorized dissemination, collection and/or use of their customers' PII as a result of the businesses' lack of reasonable and adequate security measures and practices.

148. As a direct and proximate result of Defendants' negligence *per se*, the Consumer Plaintiffs and the other Class members have suffered injury and damages as described herein.

149. Defendants' violation of Section 5 of the FTC Act thus constitutes negligence *per se* and Consumer Plaintiffs and the other Class members are entitled to recover damages in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
(Unjust Enrichment)

150. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

151. Consumer Plaintiffs and members of the Multi-State Unjust Enrichment Class, or in the alternative the statewide Unjust Enrichment Class (the "Class" as used in this count), conferred a monetary benefit on Defendants in the form of money paid for the purchase of goods from Defendants.

152. Defendants appreciate or have knowledge of the benefits conferred directly upon them by Consumer Plaintiffs and the other members of the Class.

153. Defendants knew or should have known about the Data Breach and but for their inadequate security practices, would have known about the Data Breach on its original date of occurrence.

154. Had Consumer Plaintiffs and the other Class members known about the Data Breach, they would not have shopped at Defendants' stores and would not have conferred upon Defendants monetary benefits.

155. Thus, had Consumer Plaintiffs and the other Class members been alerted to the Data Breach by Defendants, who knew or should have known, they would not have shopped at Defendants' stores and purchased goods from Defendants.

156. The financial benefits of money paid by Consumer Plaintiffs and the other Class members and the profits derived therefrom are a direct and proximate result of Defendants' unlawful and negligent practices and Defendants' failure to notify Consumer Plaintiffs and the other Class members of the Data Breach.

157. These financial benefits rightfully belong to the Consumer Plaintiffs and the other Class members and it would be inequitable under unjust enrichment principles for Defendants to retain any of the financial benefits they would not have received but-for their illegal and uncaring conduct.

158. As such, Defendants should be compelled to disgorge all inequitable proceeds to Consumer Plaintiffs and the other Class members by way of a common fund for their benefit.

159. A constructive trust should be imposed to recoup the inequitable sums received by Defendants and traceable to Consumer Plaintiffs and the other Class members.

PRAYER FOR RELIEF

Wherefore, Consumer Plaintiffs pray for a judgment:

1. Certifying the Class(es) as requested herein;

2. Awarding Consumer Plaintiffs and the proposed Class members damages;

3. Awarding restitution and disgorgement of Defendants' revenues to Consumer Plaintiffs and the proposed Class members;

4. Awarding consequential damages for time and money spent by Consumer Plaintiffs and the other members of the Class in response to Defendants' improper release and dissemination of their PII;

5. Awarding injunctive relief as permitted by law or equity, including:

   a. Enjoining Defendants from continuing the unlawful practices as set forth herein;

   b. Directing Defendants to identify, with Court supervision, victims of their conduct and pay them all money they are required to pay; and

   c. Ordering Defendants to engage in a corrective advertising campaign;

6. Awarding damages, as appropriate;

7. Awarding attorneys' fees, costs, and expenses; and

8. Providing such further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Consumer Plaintiffs hereby demand a jury trial of their claims to the extent authorized by law.

DATED: June 26, 2015

Respectfully submitted,

s/ Ben Barnow

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

Edwin J. Kilpela, Jr.
CARLSON LYNCH SWEET & KILPELA, LLP
115 Federal Street, Suite 210
Pittsburgh, PA 15212
(412) 322-9243 (p)
(412) 231-0246 (f)
ekilpela@carlsonlynch.com

Plaintiffs' Interim Co-Lead Counsel

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

Plaintiffs' Interim Liaison Counsel

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

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
(612) 339-6900 (p)
(612) 339-0981 (f)
khriebel@locklaw.com

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

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

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

Plaintiffs' Interim Executive Committee

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Consolidated Amended Class Action Complaint was served on all counsel of record via the Court's ECF filing system.

Dated: June 26, 2015

s/ Ben Barnow

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