IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

GREATER CHAUTAUQUA FEDERAL CREDIT UNION, individually and on behalf of a class of similarly situated financial institutions, Plaintiff, v. KMART CORPORATION and SEARS HOLDINGS CORPORATION, Defendants.	Case No: 15-cv-2228 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Greater Chautauqua Federal Credit Union ("GCFCU" or "Plaintiff") by its undersigned counsel, individually and on behalf of a class of similarly situated financial institutions, upon personal knowledge as to itself and its own acts, and upon information and belief and investigation by Plaintiff's counsel (which included, among other things, a review of public documents as to all other matters), brings this action against Defendants Kmart Corporation ("Kmart") and Sears Holdings Corporation ("Sears") (collectively the "Defendants") and alleges the following:

NATURE OF THE ACTION

1. This is a class action on behalf of credit unions, banks, and other financial institutions that suffered injury as a result of a security breach beginning on or around early September 2014 (hereinafter the "Kmart Data Breach"). The Kmart Data Breach compromised the names, credit and debit card numbers, card expiration dates, card verification values ("CVVs"), and other credit and debit card information of Kmart customers.

2. The Kmart Data Breach forced Plaintiff and other financial institutions to:

a. cancel or reissue any credit and debit cards affected by the Kmart Data Breach;

b. close any deposit, transaction, checking, or other accounts affected by the Kmart Data Breach, including but not limited to stopping payments or blocking transactions with respect to the accounts;

c. open or reopen any deposit, transaction, checking, or other accounts affected by the Kmart Data Breach;

d. refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Kmart Data Breach;

e. respond to a higher volume of cardholder complaints, confusion, and concern;

f. increase fraud monitoring efforts; and

g. lose revenue as a result of a decrease in card usage after the breach was disclosed to the public.

3. Defendants' failure to maintain adequate computer data security directly and proximately caused Plaintiff's injuries. Defendants failed to adequately protect customer information including credit and debit card data and personal identifying information ("PII"). Defendants failed to employ adequate security measures despite the known threat of attacks by third parties using malware and other malicious software to gather sensitive information, as has been well-publicized after data breaches at large national retail and restaurant chains in recent months including Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's and Neiman Marcus.

4. Defendants' failure to adequately secure their data was inexcusable. The Kmart Data Breach involved most of the same techniques as those used in major data breaches in the preceding months and years. Nevertheless, despite having knowledge that such data breaches were occuring, Defendants failed to adequately protect sensitive payment card information and caused damage to Plaintiff and other similarly situated financial institutions.

5. Not only did Defendants fail to prevent the intrusion, but they compounded the injury by failing to detect or notify customers of the infiltration for a period of at least five weeks.

6. According to Defendants' security experts, the Kmart data systems were infected with a form of malware that its antivirus systems failed to detect. As such, the volume of data stolen was much greater than it would have been had Defendants maintained adequate antivirus software systems to identify and eliminate the breach at the time it occurred.

7. On October 10, 2014, Kmart announced that its payment data systems had been breached.[1] In confirming the breach in a Form 8-K filing with the Securities and Exchange Commission on October 10, 2014, parent company Sears confirmed that the breach started in early September, had been going on for five weeks, and affected customers using the payment data systems at Kmart stores for the entire month of September through October 9, 2014.[2] Defendants did not disclose the scale of the breach, the number of cards compromised, or the nature of the malware used.

---

[1] *See* Alasdair James, President and Chief Member Officer at Kmart, *Kmart Investigating Payment System Intrusion* (Oct. 10, 2014), http://www.kmart.com/ue/home/10.10.14_News_Release.pdf (last accessed March 5, 2015) (hereinafter "Kmart Oct. 10 Statement").

[2] *See* Sears Holdings Corporation, SEC Form 8-K (Oct. 10, 2014), *available at* http://www.sec.gov/Archives/edgar/data/1310067/000119312514369356/d803829d8k.htm (last accessed March 5, 2015) (hereinafter "Sears Holdings Corp., SEC Form 8-K (Oct. 10, 2014)").

8. As a direct and proximate result of Defendants' negligence, vast amounts of financial and customer information was stolen from the Kmart computer network. The data stolen in the breach would allow thieves to create counterfeit copies of the stolen cards.[3] Though an investigation is still ongoing, it appears that credit and debit card data from hundreds of thousands of accounts of Defendants' Kmart customers has been stolen. Plaintiff and members of the Class have incurred and will continue to incur significant damages associated with, among other things:

a. notifying their customers of issues related to the Kmart Data Breach;

b. costs for cancelling and reissuing thousands of credit and/or debit cards;

c. costs for reimbursing their customers for fraudulent charges, including, but not limited to issuing refunds or credits to affected customers;

d. voiding deposits and transactions and closing checking or other accounts affected by the breach, including, but not limited to stopping payments or blocking transactions with respect to affected accounts;

e. handling a higher-than-usual number of customer service inquiries; and

f. conducting investigations related to the breach.

9. Plaintiff and the members of the Class seek to recover damages caused by Defendants' violations of the Illinois Personal Information Protection and Consumer Fraud Acts and the New York General Business Law, negligence, and negligent misrepresentations by omission.

[3] *See* Brian Krebs, *Malware Based Credit Card Breach at Kmart*, KrebsOnSecurity (Oct. 10, 2014), http://krebsonsecurity.com/2014/10/malware-based-credit-card-breach-at-kmart/ (last accessed March 5, 2015) (hereinafter "Brian Krebs, *Malware Based Credit Card Breach at Kmart*").

JURISDICTION AND VENUE

10. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d), in that: (a) the Class has more than 100 Class members; (b) the amount at issue exceeds five million dollars ($5,000,000.), exclusive of interest and costs; and (c) minimal diversity exists as Plaintiff and Defendants are citizens of different states. Plaintiff Greater Chautauqua Federal Credit Union is a citizen of New York. Defendant Kmart is a citizen of Michigan, where it is incorporated, and Illinois, where its principal place of business is located. Defendant Sears is a citizen of Delaware, where it is incorporated, and Illinois, where its principal place of business is located.

11. Venue in the United States District Court for the Northern District of Illinoisis appropriate, pursuant to 28 U.S.C. §1391, in that Defendants maintain their principal places of businessin this District, regularly transact business in this District, and a substantial part of the events giving rise to this claim arose in this District.

PARTIES

12. Plaintiff Greater Chautauqua Federal Credit Union is a chartered federal credit union whose main offices are located in Falconer, NY.

13. Plaintiff provided its customers with credit and/or debit cards equipped with magnetic strips containing sensitive financial data. Plaintiff's customers used these cards to engage in financial transactions at Defendants' stores.

14. As a result of the Kmart Data Breach, Plaintiff incurred damages for, among other things, the cost of replacement cards. These costs are ongoing, as Plaintiff continues to investigate fraudulent transactions caused by the data breach that have not yet been reimbursed.

15. Defendant Sears Holdings Corporation is a Delaware corporation with its principal place of business located at 3333 Beverly Road, Hoffman Estates, Illinois 60179. Sears Holdings Corporation is the parent company of Kmart and was formed in 2004 in connection with the merger of Kmart and Sears, Roebuck & Co.

16. Defendant Kmart Corporation is a Michigan corporation with its principal place of business located at 3333 Beverly Road, Hoffman Estates, Illinois 60179. Kmart operates a chain of retail stores that sell a wide variety of merchandise, including home appliances, consumer electronics, home goods, apparel, grocery and household, pharmacy and drugstore items. Kmart operates approximately 1,077 stores in the United States.

FACTUAL ALLEGATIONS

Background on Electronic Debit and Credit Card Transactions

17. Plaintiff and the members of the Class are financial institutions that issue payment cards (*e.g.*, debit or credit cards branded with the VISA or MasterCard logo) to their customers. Plaintiff's customers used these cards to make purchases at Kmart stores during the period of the Kmart Data Breach.

18. Kmart stores accept customer payment cards for the purchase of goods and services. At the point of sale ("POS"), these cards are swiped on a POS terminal, and either a personal identification number (or some other confirmation number) is entered or a receipt is signed to finish the transaction on behalf of the customer.

19. A typical credit or debit card transaction made on a credit card network is processed through a merchant (where the initial purchase is made), an acquiring bank (which is typically a financial institution that contracts with a merchant to process its credit card and debit card transactions and is a member of the credit card associations) a processor, and an issuer

(which is a financial institution like Plaintiff and members of the proposed Class that issues credit cards and debit cards to consumers and is a member of the credit card associations). When a purchase is made using a credit card or debit card on a credit card network, the merchant seeks authorization from the issuer for the transaction. In response, the issuer informs the merchant whether it will approve or decline the transaction. Assuming the transaction is approved, the merchant processes the transaction and electronically forwards the receipt directly to the acquiring bank. The acquiring bank then pays the merchant, forwards the final transaction data to the issuer, and the issuer reimburses the acquiring bank. The issuer then posts the charge to the consumer's credit card or debit card account.

20. Given the extensive network of financial institutions involved in these transactions and the sheer volume of daily transactions using credit and debit cards, financial institutions and credit card processing companies have issued rules and standards governing the basic measures and protections that merchants must take to ensure consumers' valuable data is protected.

21. First, the card processing networks issue regulations ("Card Operating Regulations") that are enforceable upon Defendants as a condition of Defendants' contract with the acquiring bank. The Card Operating Regulations generally prohibit Defendants (or any merchant) from disclosing any cardholder account numbers, personal information, magnetic stripe information, or transaction information to third parties other than the merchant's agent, the acquiring bank, or the acquiring bank's agents. Under the Card Operating Regulations, Defendants are ***required*** to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and protect it from unauthorized disclosure.

22. Similarly, the Payment Card Industry Data Security Standards ("PCI DSS") is a list of 12 information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires merchants like Defendants to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

23. The 12 requirements of the PCI DSS are:

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data

4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs

6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know

8. Identify and authenticate access to system components

9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel.[4]

24. Defendants were at all times fully aware of their data protection obligations, which emanated from their participation in the payment card processing networks and their daily collection and transmission of tens of thousands of sets of payment card data.

25. As a result of their participation in the payment card processing networks, Defendants knew that their customers and the financial institutions which issued the payment cards to the customers were trusting that Defendants would keep their customers' sensitive financial information secure from data thieves.

26. Furthermore, Defendants knew that if they failed to secure their customers' sensitive financial information, the financial institutions issuing the payment cards to their customers, *i.e.*, Plaintiff and other Class members, would suffer harm by having to notify customers, close out and open new customer accounts, reissue customers cards and/or refund customers' losses resulting from the unauthorized use of their accounts, and suffer lost revenues as a result of decreased usage of their customers' debit/credit cards.

27. Plaintiff believes that the deficiencies in Kmart's security system included a lack of basic security measures that IT professionals would identify as problematic.

[4] The PCI DSS 12 core security standards can be found at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf, at pg. 5 (last visited March 5, 2015).

28. Specifically, some of the security flaws identified in the Kmart Data Breach were explicitly highlighted by VISA as early as 2009, when it issued a Data Security Alert describing the threat of RAM scraper malware.[5] The report instructs companies to:

- "Secure remote access connectivity;"
- "Implement a secure network configuration, including egress and ingress filtering to ***only*** allow the ports/services necessary to conduct business" (emphasis in original) (*i.e.*, segregate networks);
- "[A]ctively monitor logs of network components, including IDS [intrusion detection systems] and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses;"
- "Encrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit;" and
- "Work with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration."[6]

29. Plaintiff believes that Kmart's security flaws run afoul of industry best practices and standards. Specifically, the security practices in place at Kmart are in direct conflict with the PCI DSS and the 12 PCI DSS core security standards. All merchants are required to adhere to the PCI DSS as members of the payment card industry.

---

[5] The report can be found at: https://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf (last visited March 5, 2015).

[6] *Id.*

30. As a result of industry warnings, industry practice, the PCI DSS requirements, and multiple well-documented data breaches, Defendants were aware of the risks associated with failing to ensure that their IT systems were adequately secured.

The Kmart Data Breach: the Result of Lax Anti-Virus Standards

31. On information and belief, Kmart's information technology hardware and personnel are headquartered in Hoffman Estates, Illinois. On information and belief, the physical servers on which the malware was inserted are located there, as well as the technologies employed to prevent such attacks. Additionally, on information and belief, the key officers and employees responsible for developing and implementing Kmart's information technology security are located in Hoffman Estates, Illinois.

32. Hackers infiltrated Kmart's payment data systems with malware that its systems could not detect because its anti-virus system had not been updated to include such threats.[7] POS registers at its stores were infected with software that stole customer credit and debit card information from the registers. Kmart reported that credit and debit card numbers were compromised in the breach, but it has still not informed its customers or Plaintiff of the scope of the breach.

33. Kmart claims that only "track 2" data from customer credit and debit cards has been compromised, which includes the cardholder account number, country code, expiration date, some encrypted PIN information and other discretionary data. Kmart claims that the breach did not include customer names, physical addresses, email addresses, social security numbers,

[7] *See* Kmart Oct. 10 Statement.

unencrypted PINs, or other sensitive information. However, Kmart has acknowledged that "the information stolen would allow thieves to create counterfeit copies of the stolen cards."[8]

34. Defendants failed to maintain and update anti-virus software capable of detecting malware threats despite ongoing and continued hacking at retailers throughout the country. This type of security maintenance is a basic part of running a secure network and protecting card member data.

35. The failure to utilize adequately updated anti-virus and anti-malware systems allowed hackers to infiltrate the POS system such that customer credit and debit card information could be captured.

36. Plaintiff believes that Kmart's IT department and executives were aware that the company was vulnerable to a breach of customer financial information and they were aware of countermeasures on the market which could reduce or eliminate the ability of hackers to steal customer card data from POS terminals. Nevertheless, Defendants were negligent in that they failed to adequately protect the credit and debit card data and prevent the Kmart Data Breach.

37. Defendants were not only aware of the threat of data breaches generally, but were aware of the specific danger of malware infiltration. Malware has been used to access POS terminals since at least 2011, and specific types of malware, including RAM scraper malware, have been used recently to infiltrate large retailers such as Target, Sally Beauty, Neiman Marcus, Michaels Stores, and SuperValu. As a result, Defendants were aware that malware is a real threat and is a primary tool of infiltration used by hackers.

38. Defendants received additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of

[8] *See* Brian Krebs, *Malware Based Credit Card Breach at Kmart*.

Homeland Security, which alerted retailers to the threat of POS malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of POS malware, which was updated on August 27, 2014.[9] Additionally, the Homeland Security Department and the Secret Service issued a report warning retailers to check their in-store cash register systems for a set of malware that could evade detection of antivirus products. Kmart should have taken action to protect and ensure that its customers' information would not continue to be available to hackers and identity thieves, but Kmart chose not to do so.

39. Despite the fact that Defendants were put 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 basic infirmities associated with the Kmart security systems, they still failed to make necessary changes to their security practices and protocols.

40. Defendants knew or should have known that failing to protect customer card data would cause harm to the card-issuing institutions such as Plaintiff and the Class because such issuers are financially responsible for fraudulent card activity and must incur significant costs to prevent additional fraud.

41. Indeed, Defendants' public statements to customers after the data breach plainly indicate that Defendants believe that card-issuing institutions should be responsible for fraudulent charges on cardholder accounts resulting from the data breach.[10] While Kmart has made free credit monitoring available to consumers affected by the data breach, it has made no

[9] *See* United States computer Emergency Readiness Team, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (Aug. 27, 2014), https://www.us-cert.gov/ncas/alerts/TA14-212A (last accessed March 5, 2015).

[10] *See* Kmart Oct. 10 Statement ("[T]he policies of the credit card companies state that customers have zero liability for any unauthorized charges if they report them in a timely manner . . . . If customers see any sign of suspicious activity, they should immediately contact their card issuer.").

overtures to the card-issuing institutions that are left to absorb their damages as a result of the breach.

42. Defendants, at all times relevant to this action, had a duty to Plaintiff and members of the Class to, and represented that they would:

a. properly secure payment card magnetic stripe information at the point of sale and on Defendants' internal networks;

b. encrypt payment card data using industry standard methods;

c. properly update and maintain anti-virus and anti-malware software;

d. use readily available technology to defend its POS terminals from well-known methods of attack; and

e. act reasonably to prevent the foreseeable harms to Plaintiff and the Class which would naturally result from payment card data theft.

43. Defendants negligently allowed payment card magnetic stripe information to be compromised by failing to take reasonable and prudent steps against an obvious threat.

44. As a direct and proximate result of the events detailed herein, Plaintiff and members of the Class have been injured by, among other things, incurring costs to protect their customers' financial information by cancelling and reissuing cards with new account numbers and magnetic stripe information.

45. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the Class, which were proximately caused by Defendants' negligence. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

Plaintiff and the Class Have Been Damaged as a Result of Defendants' Wrongdoing

46. Due to Defendants' failure to safeguard customer information, Plaintiff has been forced to cancel and reissue hundreds of cards and incur related costs for notification and re-issuance of cards to its clients.

47. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the proposed Class. Moreover, as a result of the events detailed herein, Plaintiff and members of the proposed Class suffered losses resulting from Kmart's Data Breach related to the need to:

a. cancel or reissue any credit and debit cards affected by the Kmart Data Breach;

b. close any deposit, transaction, checking, or other accounts affected by the Kmart Data Breach, including but not limited to stopping payments or blocking transactions with respect to the accounts;

c. open or reopen any deposit, transaction, checking, or other accounts affected by the Kmart Data Breach;

d. refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Kmart Data Breach;

e. respond to a higher volume of cardholder complaints, confusion, and concern; and

f. increase fraud monitoring efforts.

48. Plaintiff has incurred thousands of dollars of fraud losses. Plaintiff has also incurred internal costs, such as:

a. employee time and overhead charges related to the reissuance of hundreds of cards;

b. providing responses to customer inquiries;

c. notifying customers; and

d. dealing with fraudulent charges and crediting its customer's accounts.

49. These costs and expenses will continue to accrue as additional fraud alerts and fraud charges are discovered and occur.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings Counts I, II, IV, and V in this action individually and on behalf of all other financial institutions similarly situated pursuant to Fed. R. Civ. P. 23. The proposed class is defined as:

> All Financial Institutions including, but not limited to, banks and credit unions in the United States (including its Territories and the District of Columbia) that issue payment cards, including credit and debit cards, or perform, facilitate, or support card issuing services, whose customers made purchases from Kmart stores from September 1, 2014 to October 9, 2014 (the "National Class").

Excluded from the National Class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

51. Plaintiff brings Count III individually and on behalf of all other similarly situated New York financial institutions pursuant to Fed. R. Civ. P. 23. The proposed class is defined as:

> All Financial Institutions including, but not limited to, banks and credit unions in the State of New York that issue payment cards, including credit and debit cards, or perform, facilitate, or support card issuing services, whose customers made purchases from Kmart stores from September 1, 2014 to October 9, 2014 (the "New York State Class").

Excluded from the New York State Class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

52. The National Class and New York State Class are referred to collectively herein as "the Class."

53. Plaintiff is a member of the Class it seeks to represent. The Class is so numerous that joinder of all members is impracticable. The members of the Class are readily ascertainable. Plaintiff's claims are typical of the claims of all members of the Class. The conduct of Defendants has caused injury to Plaintiff and members of the Class. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendants. Plaintiff will fairly and adequately represent the interests of the Class. Defendants have acted or refused to act on grounds that apply generally to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole. Plaintiff is represented by experienced counsel who are qualified to litigate this case.

54. Common questions of law and fact predominate over individualized questions. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. There are questions of law and fact common to all members of the Class, the answers to which will advance the resolution of the claims of the Class members and that include, without limitation:

a. whether Defendants failed to provide adequate security and/or protection for their computer systems containing customers' financial and personal data;

b. whether the conduct of Defendants resulted in the unauthorized breach of their computer systems containing customers' financial and personal data;

c. whether Defendants failed to properly maintain updated anti-virus and anti-malware systems;

d. whether Defendants' actions were negligent;

e. whether Defendants owed a duty to Plaintiff and the Class;

f. whether the harm to Plaintiff and the Class was foreseeable;

g. whether Plaintiff and members of the Class are entitled to injunctive relief; and

h. whether Plaintiff and members of the Class are entitled to damages and the measure of such damages.

COUNT ONE
VIOLATION OF THE ILLINOIS PERSONAL INFORMATION PROTECTION ACT ("PIPA"), 815 Ill. Comp. Stat. 530/10 *et seq.*
(On behalf of the National Class)

55. Plaintiff incorporates paragraphs 1-54 as if fully set forth herein.

56. The Illinois Personal Information Protection Act includes a requirement that a "data collector" timely notify Illinois residents of any breach of security "in the most expedient time possible and without unreasonable delay." Ill. Comp. Stat. 530/10(a). Such notice must include "the toll-free numbers and addresses for consumer reporting agencies," "the toll-free number and website address for the Federal Trade Commission, and "a statement that the individual can obtain information from these sources about fraud alerts and security freezes." *Id.*

57. In the alternative, a "data collector that maintains or stores" personal information subject to a breach must notify the licensee of that information "immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by

an unauthorized person." Ill. Comp. Stat. 530/10(b). Notice also includes a requirement to "cooperate with . . . licensee in matters related to the breach," including informing the licensee of steps taken or planned relating to the breach.

58. Defendants are "data collectors" under PIPA.

59. Plaintiff is a "licensee" of computerized data that includes personal information under PIPA by virtue of its relationships with its bank customers.

60. Defendants failed to timely notify affected customers of the nature and extent of the security breach. There were five weeks between when the breach started and when Kmart announced it had occurred on its website or filed an updated Form 8-K with the SEC.

61. Defendants failed to notify Plaintiff and the Class of the breach of security in conformance with PIPA. To date, Plaintiff has received neither notice of the breach from Defendants nor been informed of Defendants' next steps in dealing with the breach.

62. Additionally, Defendants' public notice via the October 10 Statement and a filed Form 8-K was inadequate. The October 10 Statement did not contain toll-free numbers for either consumer reporting agencies or the Federal Trade Commission, did not contain a statement that individuals could obtain fraud alert or security freeze information from those sources, and did not contain address information for consumer reporting agencies.

63. A violation of the statute constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Act ("ICFA").

64. This unlawful practice and the underlying transaction, namely the data breach, occurred primarily and substantially in Illinois.

65. Defendants intended for Plaintiff and the Class to rely on these unlawful practices, and in fact knew that it was Plaintiff and the Class, not Defendants, that would pay for damages incurred by a security breach of the sort that in fact occurred.

66. The unlawful conduct occurred in the course of conduct involving trade or commerce because Plaintiff and the Class and Defendants have a contractual relationship related to the use and acceptance of credit and debit cards at Kmart stores.

67. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class have suffered substantial losses as detailed herein.

COUNT TWO
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS ACT ("ICFA"), 815 Ill. Comp. Stat. 505/1 *et seq*.
(On behalf of the National Class)

68. Plaintiff incorporates paragraphs 1-54 as if fully set forth herein.

69. Defendants failed to follow security protocols. To wit, Defendants failed to heed the 2009 VISA Data Security Alert describing the threat of RAM scraper malware and failed to secure remote access connectivity or otherwise implement adequate security procedures. Additionally, the security practices in place at Kmart directly conflict with the Payment Card Industry Data Security Standards and requirements three and five of the 12 PCI DSS core security standards, and Defendants failed to change the defective security protocols at Kmart and implement proper security procedures in line with their PCI DSS obligations.

70. These actions collectively constitute an "unfair practice" under the ICFA because of their substantial injury to other companies and consumers.

71. This "unfair practice" and the underlying transaction, namely the data breach, occurred primarily and substantially in Illinois.

72. Defendants intended for Plaintiff and the Class to rely on these unfair practices, and in fact knew that it was Plaintiff and the Class, not Defendants, that would pay for damages incurred by a security breach of the sort not protected against.

73. The unfair conduct occurred in the course of conduct involving trade or commerce because Plaintiff and the Class and Defendants have a contractual relationship related to the use and acceptance of credit and debit cards at Kmart stores.

74. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class have suffered substantial losses as detailed herein.

75. Plaintiff's and the other Class members' injuries were proximately caused by Defendants' unfair practice, which was conducted with reckless indifference toward the rights of others such that an award of punitive damages is appropriate

COUNT THREE
VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW
(On behalf of the New York State Class)

76. Plaintiff incorporates paragraphs 1-54 as if fully set forth herein.

77. New York General Business Law ("GBL") § 349 makes unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce." N.Y. Gen. Bus. Law § 349.

78. Defendants' transactions with Plaintiff and the New York State Class as described herein constitute the "conduct of any trade or commerce" within the meaning of GBL § 349.

79. Defendants, in the normal course of its business, collected customer information, including debit and credit card information and PII.

80. Defendants violated GBL § 349 by failing to properly implement adequate, commercially reasonable security measures to protect customers' debit and credit card information and PII, by failing to warn shoppers that their information was at risk, and by failing

to immediately notify affected customers of the nature and extent of the security breach. Defendants misrepresented the safety and security of their payment systems.

81. Plaintiff and the other members of the New York State Class have suffered injury in fact and substantial losses as detailed herein, including lost money and property, as a result of Defendants' violations of GBL § 349.

82. Plaintiff's and the other Class members' injuries were proximately caused by Defendants' fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

COUNT FOUR
NEGLIGENCE
(On behalf of the National Class)

83. Plaintiff incorporates and re-alleges paragraphs 1-54 as if fully set forth herein.

84. Defendants owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining and processing Plaintiff's customers' personal and financial information.

85. Defendants owed a duty to Plaintiff and the Class to provide adequate security to protect their mutual customers' personal and financial information.

86. Defendants breached their duties by (1) allowing a third-party intrusion into their computer systems; (2) failing to protect against such an intrusion; (3) failing to maintain updated anti-virus and anti-malware software necessary to prevent such an intrusion; and (4) allowing the personal and financial information of customers of Plaintiff and the Class to be accessed by third parties on a large scale.

87. Defendants knew or should have known of the risk that their POS terminals could be infiltrated using methods similar or identical to those previously used against major retailers in recent months and years.

88. Defendants knew or should have known that their failure to take reasonable measures to protect their POS terminals against obvious risks would result in harm to Plaintiff and the Class.

89. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and the Class have suffered substantial losses as detailed herein.

COUNT FIVE
NEGLIGENT MISREPRESENTATION AND/OR OMISSION
(On behalf of the National Class)

90. Plaintiff incorporates and re-alleges paragraphs 1-54 as if fully set forth herein.

91. Through their acceptance of credit and debit payment cards and participation in the payment card processing system at Kmart stores, Defendants held themselves out to Plaintiff and the Class as possessing and maintaining adequate data security measures and systems that were sufficient to protect the personal and financial information of shoppers using credit and debit cards issued by Plaintiff and the Class.

92. Defendants further represented that they would secure and protect the personal and financial information of shoppers using credit and debit cards issued by Plaintiff and the Class by agreeing to comply with both Card Operating Regulations and the PCI DSS.

93. Defendants knew or should have known that they were not in compliance with the requirements of Card Operating Regulations and the PCI DSS.

94. Defendants knowingly and deliberately failed to correct material weaknesses in their data security systems and procedures that good faith required them to disclose to Plaintiff and the Class.

95. A reasonable business would have taken necessary steps to prevent the material weaknesses in its data security measures and systems to Plaintiff and the Class.

96. Defendants' failure to disclose their inadequate security systems was particularly egregious in light of the highly publicized, similar data breaches at other national retailers in the months preceding the Kmart Data Breach.

97. As a direct and proximate result of Defendants' negligent misrepresentations and omissions, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendants and in favor of Plaintiff and the Class and award the following relief:

A. That this action be certified as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as representative of the Class and Plaintiff's counsel as counsel for the Class;

B. Monetary damages;

C. Injunctive Relief;

D. Reasonable attorneys' fees and expenses, including those related to experts and consultants;

E. Costs;

F. Pre- and post-judgment interest; and

G. Such other relief as this Court may deem just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff, individually and on behalf of the Class, demands a trial by jury for all issues so triable.

DATED: March 13, 2015

Respectfully submitted,

/s/ Katrina Carroll
Katrina Carroll, Esq.
kcarroll@litedepalma.com
Kyle A. Shamberg, Esq.
kshamberg@litedepalma.com
LITE DEPALMA GREENBERG, LLC
211 W. Wacker Drive
Suite 500
Chicago, Illinois 60606
312.750.1265

James J. Pizzirusso, Esq.
jpizzirusso@hausfeld.com
Swathi Bojedla, Esq.
sbojedla@hausfeld.com
HAUSFELD LLP
1700 K Street, NW
Suite 650
Washington, DC 20006
202.540.7200

Arthur N. Bailey, Esq.
artlaw@windstream.net
ARTHUR N. BAILEY & ASSOCIATES
111 West Second Street
Jamestown, NY 14701
716.664.2967

Attorneys for Plaintiff and the Putative Class