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

FIRST NBC BANK, individually and on behalf of a class of similarly situated financial institutions, Plaintiff, v. KMART CORPORATION and SEARS HOLDINGS CORPORATION, Defendants.	Case No: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff First NBC Bank ("Plaintiff"), through its undersigned counsel, individually and on behalf of a class of similarly situated financial institutions, files this Class Action Complaint against Defendants Kmart Corporation ("Kmart") and Sears Holdings Corporation ("Sears") (collectively "Defendants"), and states the following:

INTRODUCTION

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 that compromised the names, credit and debit card numbers, card expiration dates, card verification values ("CVVs"), and other credit and debit card information of customers of Defendants' Kmart brand retail stores (hereinafter, the "Kmart Data Breach").

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; and (f) increase fraud monitoring efforts.

3. In addition, the Kmart Data Breach caused Plaintiff and the members of the class to lose revenue as a result of a decrease in card usage after the breach was disclosed to the public.

4. As alleged herein, the injuries to Plaintiff and the Class were directly and proximately caused by Defendants' failure to maintain adequate computer data security for customer information, including credit and debit card data and personally identifying information. Defendants failed to take steps to employ adequate security measures despite well-publicized data breaches at large, national retail and restaurant chains in recent months, including Target, Home Depot, Sally Beauty, Harbor Freight Tools, and P.F. Chang's.

5. The failure of Defendants to adequately secure their data networks was particularly inexcusable given the fact that the infiltration underlying the Kmart Data Breach involved mostly the same techniques as those used in major data breaches in the preceding months and years, including the well-publicized data breaches at Target and Home Depot retail stores. Nevertheless, despite having knowledge that such data breaches were occurring throughout the retail industry, Defendants failed to properly defend sensitive payment card information from what is now a well-known, preventable breach.

6. In addition to failing to prevent the intrusion in the first instance, Defendants compounded the injury by failing to detect or notify customers of the infiltration for a period of at least five weeks. According to the security experts Defendants worked with in detecting the breach, the Kmart store payment data systems were infected with a form of malware that its

antivirus systems failed to detect. Therefore the volume of data stolen was much greater than it would have been had Defendants maintained sufficient malware monitoring anti-virus systems to identify and eliminate the breach as it was occurring.

7. As a direct and proximate consequence of Defendants' negligence, vast amounts of customer information were stolen from the Kmart computer network. Though an investigation is still ongoing, it appears that hundreds of thousands of Defendants' Kmart customers have had their credit and debit numbers compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Moreover, Plaintiff and members of the Class have incurred and will continue to incur significant costs associated with, among other things, notifying their customers of issues related to the Kmart Data Breach, closing out and opening new customer accounts, reissuing customers' cards, and/or refunding customers' losses resulting from the unauthorized use of their accounts.

8. Plaintiff and the members of the Class seek to recover damages caused by Defendants' negligence and negligent misrepresentations by omission.

JURISDICTION AND VENUE

9. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class defined below, many of which are citizens of a different state than Defendant, including named Plaintiff First NBC Bank, which is a citizen of Louisiana. 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.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because Defendants reside in this judicial district, regularly transact business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

PARTIES

11. Plaintiff First NBC Bank is a Louisiana bank headquartered at 210 Baronne Street, New Orleans, Louisiana.

12. Defendant Kmart Corporation is a Michigan corporation with a 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 & household, pharmacy and drugstore items. Kmart operates approximately 1,077 stores in the United States.

13. Defendant Sears Holdings Corporation is a Delaware corporation with a 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 and Co.

FACTUAL BACKGROUND

Background on Electronic Debit and Credit Card Transactions

14. Plaintiff and the members of the Class are financial institutions that issue payment cards[1] to their customers.

15. 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

[1] These cards include, for example, debit or credit cards branded with the VISA or MasterCard logo.

personal identification number (or some other confirmation number) is entered, or a receipt is signed to finish the transaction on behalf of the customer.

16. A basic description of the various steps necessary to execute a credit/debit card transaction is as follows: 1) after the credit/debit card is swiped, the merchant (*e.g.*, Kmart) uses one of several payment processing networks (*e.g.*, Visa or MasterCard) to transmit a request for authorization to the institution that issued the payment card (*e.g.*, Plaintiff); 2) the issuing institution authorizes the payment and the merchant electronically forwards a receipt of the transaction to another financial institution known as the "acquiring bank," which contracts with the merchant to process credit and debit card transactions on the merchant's behalf; 3) the acquiring bank forwards the funds to the merchant to satisfy the transaction, and is then reimbursed by the issuing financial institution (*e.g.*, Plaintiff); and 4) finally, the issuing institution posts the debit or credit transaction to its customer's account.

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

18. First, the debit and credit card companies issue regulations ("Card Operating Regulations") that are enforceable upon Defendants as a condition of Defendants' contract with its 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. Notably, 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.

19. Similarly, the Payment Card Industry Data Security Standards ("PCI DSS") is a list of twelve 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.

20. The twelve requirements of the PCI DSS are:

Build and Maintain a Secure Network

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 and sensitive information 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[2]

21. Defendants were at all times fully aware of their data protection obligations for Kmart stores in light of their participation in the payment card processing networks and their daily collection and transmission of tens of thousands of sets of payment card data.

22. Furthermore, Defendants knew that because they accepted payment cards at Kmart stores containing sensitive financial information, customers and financial institutions such as Plaintiff were entitled to, and did, rely on Defendants to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

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

23. On October 10, 2014, Kmart announced that its Information Technology team had detected Kmart's payment data systems had been breached.[3] In confirming the breach in an 8-K filing on October 10, 2014, Holdings announced 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 all of the month of September through October 9, 2014.

---

[2] The PCI DSS 12 core security standards can be found at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf, at 5 (last visited Dec. 8, 2014).

[3] *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 Dec. 8, 2014).

24. On information and belief, Kmart's information technology hardware and personnel are headquartered in Hoffman Estates, Illinois. Thus, 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.

25. 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.[4] POS registers at its stores were infected with software that stole customer credit and debit card information from the registers. Based on the investigation, Kmart believes that credit and debit card numbers were compromised in the breach, but has still not yet informed its customers or the Plaintiffs of the scope of the breach.

26. While 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, and did not include customer names, physical addresses, email addresses, social security numbers, unencrypted PINs or other sensitive information, Kmart has acknowledged that "the information stolen would allow thieves to create counterfeit copies of the stolen cards."[5]

---

[4] *See* Alasdair James, President and Chief Member Officer at Kmart, *Kmart Investigating Payment System Breach* (Oct. 10, 2014), http://www.kmart.com/en_us/dap/statement1010140.html?adcell=hpnewsrelease (last accessed Dec. 8, 2014) (hereinafter "Kmart Oct. 10 Statement").

[5] *See* Brian Krebs, *Malware Based Credit Card Breach at Kmart*, KREBS ON SECURITY (Oct. 10, 2014), http://krebsonsecurity.com/2014/10/malware-based-credit-card-breach-at-kmart/ (last accessed Dec. 8, 2014).

27. Upon information and belief, 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 an elementary and basic part of running a secure network and protecting card member data.

28. 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.

29. Upon information and belief, Kmart's IT department and executives were aware that the company was vulnerable to a breach of the same nature as the one directed against Target in late 2013, and to numerous other retailers in 2014, 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 did not act in a reasonable, timely fashion to prevent the Kmart Data Breach.

30. The deficiencies in Kmart's security system include a lack of elementary security measures that even the most inexperienced IT professional could identify as problematic.

31. Had Kmart remedied the glaring deficiencies in its IT systems, it could have prevented the Kmart Data Breach because virtually all data breaches are preventable. In fact, the Online Trust Alliance, a non-profit organization whose mission is to enhance online trust, user empowerment and innovation, in its 2014 annual report, estimated that 740 million records were stolen in 2013 and that 89% of data breaches occurring in that year were avoidable.

32. The security flaws outlined above, along with many others, were explicitly highlighted by VISA, as early as 2009, when it issued a Data Security Alert describing the threat

of RAM scraper malware.[6] The report instructs companies to "secure remote access connectivity," "implement 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 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."

33. In addition to ignoring explicit warnings from VISA, Kmart's security flaws also run afoul of industry best practices and standards. More specifically, the security practices in place at Kmart are in stark contrast and directly conflict with the Payment Card Industry Data Security Standards and requirements three and five of the twelve PCI DSS core security standards. All merchants are required to adhere to the PCI DSS as members of the payment card industry.

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

35. 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,

[6] The report can be found at: https://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf (last visited Sept. 9, 2014).

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.

36. Defendants received additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of 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.[7]

37. 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 elementary infirmities associated with the Kmart security systems, they still failed to make necessary changes to their security practices and protocols.

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

39. 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.[8] While Kmart has

[7] *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 Dec. 8, 2014).

[8] *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.").

made free credit monitoring available to consumers affected by the data breach, it has made no overtures to the card-issuing institutions that are left to pay for damages as a result of the breach.

40. Defendants, at all times relevant to this action, had a duty to Plaintiff and members of the Class to: (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 available technology to defend its POS terminals from well-known methods of invasion; and (e) act reasonably to prevent the foreseeable harms to Plaintiff and the Class which would naturally result from payment card data theft.

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

42. As a result of the events detailed herein, Plaintiff and members of the Class have been and continue to be forced to protect their customers and avoid fraud losses by cancelling and reissuing cards with new account numbers and magnetic stripe information.

43. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the Class, all of which were proximately caused by Defendants' negligence. As a result of the events detailed herein, Plaintiff and members of the Class suffered losses resulting from the Kmart Data Breach related to: (a) reimbursement of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as cancelling compromised cards and purchasing and mailing new cards to their customers.

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

CLASS ACTION ALLEGATIONS

45. Plaintiff brings 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 "Class").

46. Plaintiff is a member of the Class it seeks to represent.

47. The Class is so numerous that joinder of all members is impracticable.

48. The members of the Class are readily ascertainable.

49. Plaintiff's claims are typical of the claims of all members of the Class.

50. The conduct of Defendants has caused injury to Plaintiff and members of the Class in substantially the same ways.

51. 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.

52. Plaintiff will fairly and adequately represent the interests of the Class.

53. 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.

54. Plaintiff is represented by experienced counsel who are qualified to litigate this case.

55. 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.

56. 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 its computer systems containing customers' financial and personal data;

b) Whether the conduct of Defendants resulted in the unauthorized breach of its 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.*

57. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

58. 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.*

59. 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.

60. Defendants are "data collectors" under PIPA.

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

62. 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 8-K with the SEC.

63. 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.

64. Additionally, Defendants' public notice via the October 10 Statement and a filed 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.

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

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

67. 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.

68. 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.

69. 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*.

70. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

71. 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 twelve 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.

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

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

74. 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.

75. 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.

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

COUNT THREE
NEGLIGENCE

77. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

78. 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.

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

80. 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; (4) allowing the personal and financial information of customers of Plaintiff and the Class to be accessed by third parties on a large scale.

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

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

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

COUNT FOUR
NEGLIGENT MISREPRESENTATION AND/OR OMISSION

84. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

85. 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.

86. 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.

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

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

89. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to Plaintiff and the Class.

90. 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.

91. 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: December 16, 2014

Respectfully submitted,

By: /s/ Lori A. Fanning

Marvin A. Miller
Lori A. Fanning
MILLER LAW LLC
115 S. LaSalle Street, Suite 2910
Chicago, IL 60603
Tel: (312) 332-3400
Fax: (312) 676-2676
mmiller@millerlawllc.com
lfanning@millerlawllc.com

Arthur M. Murray
Stephen B. Murray
Korey A. Nelson
MURRAY LAW FIRM
(all to be admitted *pro hac vice*)
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Tel: (504) 525-8100
Fax: (504) 584-5249
amurray@murray-lawfirm.com
smurray@murray-lawfirm.com
knelson@murray-lawfirm.com

Gary F. Lynch
Edwin J. Kilpela
Jamisen Etzel
(all to be admitted *pro hac vice*)
CARLSON LYNCH SWEET & KILPELA, LLP
PNC Park
115 Federal Street, Suite 210
Pittsburgh, PA 15212
Tel: (412) 322-9243
Fax: (412) 231-0246
glynch@carlsonlynch.com
ekilpela@carlsonlynch.com
jetzel@carlsonlynch.com

Karen Hanson Riebel
Heidi M. Silton
Kate M. Baxter-Kauf
(all to be admitted *pro hac vice*)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 339-0981
khriebel@locklaw.com
hmsilton@locklaw.com
kmbaxter-kauf@locklaw.com

Attorneys for Plaintiff