

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TRUSTMARK NATIONAL BANK and
GREEN BANK, N.A., on behalf of themselves
and all other similarly situated institutions,

CASE NO.: 14-CV-2069

Plaintiff,

v.

TARGET CORPORATION, and
TRUSTWAVE HOLDINGS, INC.

Defendants.

CLASS ACTION COMPLAINT

Panagiotis V. Albanis
MORGAN & MORGAN
12800 University Drive, Suite 600
Fort Meyers, Florida 33907
(239) 432-6605 (telephone)
(239) 433-6836 (facsimile)

Bruce W. Steckler (*Pro Hac Vice* Admission Pending)
STECKLER LAW, LLP
12720 Hillcrest Road, Suite 1045
Dallas, Texas 75230
(972) 387-4040 (telephone)
(972) 387-4041 (facsimile)

Kenneth C. Johnston (*Pro Hac Vice* Admission Pending)
Robert W. Gifford (*Pro Hac Vice* Admission Pending)
David M. Clem (*Pro Hac Vice* Admission Pending)
KANE RUSSELL COLEMAN & LOGAN PC
3700 Thanksgiving Tower
1601 Elm Street
Dallas, Texas 75201
(214) 777-4200 (telephone)
(214) 777-4299 (facsimile)

**ATTORNEYS FOR PLAINTIFFS TRUSTMARK
NATIONAL BANK and GREEN BANK, N.A.**

TABLE OF CONTENTS

I. PRELIMINARY STATEMENT 1

II. INTRODUCTION 1

III. JURISDICTION AND VENUE..... 2

IV. PARTIES..... 2

V. CLASS ACTION ALLEGATIONS 3

VI. FACTUAL STATEMENT 6

 A. Background: The Anatomy of a Payment Card Transaction 6

 B. Target Falsely Assured Trustmark And Its Customers That Target’s Computer Network and Point Of Sale Systems Complied With Industry Standards For Protecting Customers’ Confidential Payment Information. 7

 i. Target assured customers that it would protect their personal payment information. 7

 ii. The industry standards for data protection are strong—if followed. 7

 C. Warning Signs: Repeated Breaches From 2007 to 2012 Put Target On Notice That Its POS Systems Were Vulnerable. 12

 D. Black Friday 2013: The Target Data Breach..... 16

 i. Hackers infiltrate Target's POS systems and steal payment information..... 16

 ii. Identity thieves begin selling and using the stolen Payment Card information. 18

 E. The Data Breach Occurred Because Target Did Not Meet Industry Standards. 21

 i. Target does not prioritize data safety..... 21

 ii. Target outsourced its data security obligations to Trustwave—which failed to bring Target's systems up to industry standards..... 23

 F. The Target Data Breach Was Preventable And Never Should Have Happened..... 24

 G. Target Says It Accepts Full Responsibility for the Data Breach—But Has Not Compensated Class Members. 27

 i. The damage done to the Banks and the other Class members is monumental..... 28

VII. THE TARGET BREACH CAUSED SUBSTANTIAL DAMAGE TO THE CLASS..... 30

VIII. CAUSES OF ACTION 30

 Count One Negligence (All Defendants) 30

Count Two Violations Of Minn. Stat. § 325E.64 (the "Plastic Card Act") (All Defendants)32

Count Three Violations of Minn. Stat. § 325F.69 (Deceptive Practices) (All Defendants)355

Count Four Violations of Minn. Stat. § 325F.67 (False Advertising) (Target)366

Count Five Injunctive Relief (Minn. Stat. §§ 325D.45 and 325F.70) (Target).....377

Count Six Unjust Enrichment & Good Faith Reliance (Target) 38

Count Seven Negligence Per Se (All Defendants)..... 40

Count Eight Negligent Misrepresentation (Target) 41

IX. PRAYER FOR RELIEF..... 42

X. JURY DEMAND 43

Plaintiffs Trustmark National Bank ("Trustmark") and Green Bank, N.A. ("Green Bank") (collectively, the "Banks"), individually and on behalf of all other similarly situated financial institutions, defined herein, complain of the actions of Defendants Target Corporation ("Target") and Trustwave Holdings, Inc. ("Trustwave") (collectively, "Defendants") and state the following in support thereof:

**I.
PRELIMINARY STATEMENT**

By this action, the Banks seek statutory and common-law damages caused by Defendants' failure to prevent the largest retail data breach in U.S. history. The Banks also seek a mandatory injunction compelling Defendants to protect private debit and credit card information as required by both statute and industry standards.

**II.
INTRODUCTION**

1. Target is the second largest general merchandise retailer in the United States. The Banks and Class members are financial institutions that issued MasterCard branded credit cards and debit cards (collectively, the "Payment Cards") that were compromised by an ongoing and continuous data breach within Target's point-of-sale (cash register) system and internal network of systems, from November 27, 2013 through December 15, 2013 (the "Target Data Breach" or "Data Breach").

2. As a direct and proximate result of the Data Breach, the Banks and members of the Class have incurred (and will continue to incur) damages to their businesses and property in the form of, *inter alia*, expenses to cancel and reissue the compromised Payment Cards, absorption of fraudulent charges made on the compromised Payment Cards, business destruction, lost profits

and/or lost business opportunities.

3. Because Target and Trustwave failed their duties to 110 million customers, it falls to the Banks and the other Class members to protect those customers by reissuing their credit and debit cards, and communicating with those customers to prevent fraud and repay any fraudulently-made purchases. The Banks and the other Class members have therefore been damaged by Defendants' actions and are entitled to recover those damages.

III. JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction over the Banks' claims under 28 U.S.C. § 1332(d) (CAFA), because (a) there are 100 or more members of the Class, (b) at least one member of the Class is a citizen of a state diverse from the Minnesota citizenship of Target and the Illinois citizenship of Trustwave, and (c) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs. This Court has *in personam* jurisdiction over Defendants because at all relevant times, Trustwave resided and had its headquarters in the Northern District of Illinois, and both Trustwave and Target were found within, had agents in, and conducted business in the Northern District of Illinois.

5. Accordingly, venue is proper in the Eastern Division of this District Court pursuant to 28 U.S.C. § 1391(a) and 18 U.S.C. § 1965.

IV. PARTIES

6. Plaintiff Trustmark Bank is a New York state chartered bank with principal locations in New York, New Jersey, California, Nevada, and Washington D.C., with its main office located in Manhattan, New York.

7. Plaintiff Green Bank, N.A. is a Texas state financial institution with its principal office located in Houston, Texas.

8. Defendant Target Corporation is a Minnesota corporation headquartered in Minneapolis, Minnesota and operates at more than 1800 retail locations throughout the United States and well as over the Internet. Target may be served with Summons and a copy of this Class Action Complaint and Jury Demand by serving its registered agent for service of process, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201-3136.

9. Defendant Trustwave is a Delaware corporation with its principal place of business located at 70 W. Madison St., Suite 1050, Chicago, Illinois 60602. Trustwave can be served with Summons and a copy of this Class Action Complaint and Jury Demand by serving its registered agent for service of process, Alice L. Greene at 70 W. Madison St., Suite 1050, Chicago, Illinois 60602.

V.
CLASS ACTION ALLEGATIONS

10. The Banks bring this action on their own behalf and on behalf of all other Financial Institutions similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure. The Class is defined as follows:

All banks, credit unions, financial institutions¹ and other entities in the United States that issue credit, debit or stored value cards or any other similar device that contains a magnetic stripe, microprocessor chip, or other means for storage of information (collectively, "access devices") whose customers' information was compromised due to the data breach first announced by Target on December 19, 2013, and who were damaged thereby.

¹ "Financial institution" includes any office of a bank, bank and trust, savings bank, industrial loan association, savings association, credit union, regulated lender, or other banking power.

11. The Banks are members of the Class they seek to represent.

12. This action satisfies the procedural requirements set forth in Rule 23 of the Federal Rules of Civil Procedure.

13. The conduct of Defendants has caused injury to members of the Class.

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

15. There are substantial questions of law and fact common to the Class. These questions include, but are not limited to, the following:

- a. whether Defendants failed to provide adequate security and/or protection for Target's computer systems containing customers' financial and personal data;
- b. whether Defendants' conduct resulted in the unauthorized breach of Target's computer systems containing customers' financial and personal data;
- c. whether Target improperly retained customer personal and financial information;
- d. whether Defendants disclosed (or directly or indirectly caused to be disclosed) private financial and personal information of customers;
- e. whether Defendants violated Minn. Stat. § 325E.64;
- f. whether Defendants engaged in unfair and deceptive acts or practices as set forth in Minn. Stat. § 325F.69 Subd. 1;
- g. whether Defendants engaged in false advertising as set forth in Minn. Stat. § 325F.67;
- h. whether Defendants owed a duty to the Banks and other members of the Class to use reasonable care in connection with Target's use and retention of customer data in processing credit and debit transactions;
- i. whether Defendants' breached their duties to exercise reasonable due care in obtaining, using, retaining, and safeguarding customer's personal

and financial information;

- j. whether Defendants' breach of their duties proximately caused damages to the Banks and the other members of the Class;
- k. whether the Banks and other members of the Class are entitled to compensation, damages, and/or other relief as a result of the breach of Defendants' duties alleged herein; and
- l. whether inactive relief is appropriate.

16. The Banks' claims are typical of the Class. The same events and conduct that give rise to the Banks' claims and legal theories also give rise to the claims and legal theories of the Class.

17. The Banks will fairly and adequately represent the interests of the Class. There are no disabling conflicts of interest between the Banks and the Class.

18. The Banks are members of the putative Class, possess the same interests, and suffered the same injuries as Class members, making their interests coextensive with those of the Class. The interests of the Banks and the Class are aligned so that the motive and inducement to protect and preserve these interests are the same for each.

19. Target has acted, or refused to act, in a manner and on grounds that apply generally to the Class, so that final injunctive relief is appropriate respecting Target and the Class as a whole.

20. Common questions of law and fact predominate over individualized questions.

21. A class action is superior to other methods for the fair and efficient adjudication of this controversy.

22. The Banks are represented by experienced counsel qualified to handle this case. The lawsuit will be capably and vigorously pursued by the Banks and their counsel.

VI.
FACTUAL STATEMENT

A. BACKGROUND: THE ANATOMY OF A PAYMENT CARD TRANSACTION

23. Target is the second-largest discount retail store chain in the United States. Target advertises and sells discounted merchandise to millions of consumers through its retail stores as well as over the Internet. Target's estimated annual sales exceed \$73.8 billion. Target is currently ranked 36th on the "Fortune 500" list of top US companies.

24. As with virtually all credit or debit card transactions made on a card network such as Visa or MasterCard, a debit or credit card transaction conducted at Target involves four principal actors. Specifically, the transaction is (1) processed by a merchant like Target, then (2) passed to an acquiring bank that contracts with the merchant to assist in processing the merchant's credit card and debit card transactions, then (3) handled by a payment processor, and finally (4) submitted to the financial institution—such as Plaintiffs—that issued the debit or credit card. The Banks and the other financial institutions that comprise the Class members are financial institutions that issue credit and debit cards to consumers, which Target accepts for payment.

25. When a purchase is made using a debit or credit card on a 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 (*e.g.*, Target), forwards the final transaction data to the issuer (*e.g.*, Trustmark and/or Green Bank) and the issuer reimburses the acquiring bank. The issuer then posts the charge to the consumer's debit card or credit card account.

26. Target, its acquiring bank, and various credit card companies together participate in systems whereby consumers may purchase goods from Target retail stores using their payment cards. The debit and credit card companies, including Visa and MasterCard, issue regulations that govern Target's conduct with respect to transactions and information involving their respective payment networks (the "Card Operating Regulations"). Target contractually agreed to comply with the Card Operating Regulations for the benefit of both the customers and the issuing banks like Trustmark and Green Bank. The Banks and the other Class members each have membership in the applicable credit and debit card networks.

B. TARGET FALSELY ASSURED TRUSTMARK AND ITS CUSTOMERS THAT TARGET'S COMPUTER NETWORK AND POINT OF SALE SYSTEMS COMPLIED WITH INDUSTRY STANDARDS FOR PROTECTING CUSTOMERS' CONFIDENTIAL PAYMENT INFORMATION.

i. Target assured customers that it would protect their personal payment information.

27. Target recognizes that its customers' personal identifying information ("PII") and payment information is highly confidential and must be protected from loss or theft. In fact, Target publicly touts the strength of its technology platform and the fact that Target purportedly adheres to "industry standard methods to protect [sensitive customer] information."

28. For example, according to Target's December 2013 Privacy Policy, Target "maintain[s] administrative, technical and physical safeguards to protect your [customers'] personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information."

ii. The industry standards for data protection are strong—if followed.

29. The widely-accepted data-protection standard for large retail institutions that accept payment cards is called PCI DSS. Succinctly put, PCI DSS consists of twelve general standards,

including: (i) installing and maintaining firewall(s) to protect data, (ii) protecting stored data, (iii) encrypting the transmission of payment cardholder data and sensitive information across public networks, (iv) using and regularly updating antivirus software, (v) developing and maintaining secure systems and applications, (vi) restricting physical access to cardholder data, (vii) tracking and monitoring all access to network resources and cardholder data, (viii) regularly testing security systems and processes, and (ix) maintaining a policy that addresses information security.

30. The core goal of the PCI DSS standard is to "[b]uild and maintain a secure network; 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."²

31. USA Today, among other sources, however, reported Target was likely not PCI DSS compliant because "the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days."³

32. Under PCI DSS, merchants like Target are required to encrypt customer names, payment card numbers, expiration dates, CVV codes (Card Verification Value codes), and PIN numbers ("Track Data"). According to Infonationweek.com, the Target Data Breach should never have happened.⁴ Forrester analyst John Kindervag further opined that "[t]he fact that the three-digit CVV security codes were compromised shows they were being stored. Storing CVV codes has long

² See www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

³ See <http://www.usatoday.com/story/cybertruth/2013/12/23/qa-pci-rules-could-help-stymie-target-data-thieves/4179941/>.

⁴ See <http://www.informationweek.com/security/attacks-and-breaches/target-breach-10-facts/d/d-id/1113228>.

been banned by the card brands and the PCI [Security Standards Council]."

33. The hackers could not have accessed Target's internal computer network and point-of-sale ("POS") system and stolen its customers' sensitive payment card information and PII but for Target's inadequate security protections—including its failure to comply with PCI DSS. Target failed to implement and maintain appropriate customer data security policies, procedures, protocols, and hardware and software systems to safeguard and protect the nature and scope of the payment card information and PII that was stolen and compromised.

34. At all times relevant hereto, Target was required to comply with these and other detailed requirements of the PCI DSS and Card Operating Regulations, which forbid Target from retaining or storing card magnetic stripe information subsequent to the authorization of the transaction. Target was also forbidden by the Card Operating Regulations 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. Indeed, under the Card Operating Regulations, Target was required to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information from unauthorized disclosure.

35. In addition to the PCI-DSS standards and Card Operating Regulations, Target was also required to comply with federal regulations which specifically obligated the Target to adopt a plan to prevent identity theft and ensure the safety of its customers' financial and personal data to the extent any such data was retained. *See* 16 C.F.R. Part 681. Those regulations, which are promulgated under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") and have been in force since 2010, require "creditors" and "financial institutions" with "covered accounts" to

implement programs to identify, detect, and respond to the warning signs, or “red flags,” that could indicate potential identity theft.

36. Under the relevant FACTA regulations, a "creditor" includes any entity that regularly extends or renews credit, and includes all entities that regularly permit deferred payments for goods or services, including Target. Indeed, one of Target's three lines of business is its U.S. Credit Card Segment, which Target describes in its Securities and Exchange Commission ("SEC") filings as an "important contributor to our overall profitability and engagement with our guests." Target's credit and debit card offerings, termed "REDcards," include the Target Visa Credit Card, the Target Credit Card, as well as a branded proprietary Target Debit Card.⁵ The customer credit card accounts for these products qualify as "covered accounts," which are broadly defined to include any account offered primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions.

37. To maintain the data security of these accounts and other credit transactions, federal regulations require Target to “oversee, develop and administer” a written Identity Theft Protection Program that identifies and addresses "red flags" indicating identity theft and other data security vulnerabilities that may lead to identity theft. These "Red Flag Rules" require that the identity theft protection plan include, among other things, provisions for detecting red flags, including procedures for monitoring credit transactions, as well as responding to and mitigating identity theft, and to provide appropriate staff training to ensure, compliance with the plan. Indeed, Target itself

⁵ Although Target sold its credit card portfolio to TD Bank in a transaction that closed on March 13, 2013, Target continued to perform account servicing and other functions for REDcards, and is entitled to a substantial portion of the profits generated by the Target Credit Card and Target Visa Credit Card portfolios that it sold to TD Bank Group. Accordingly, under the relevant regulations, Target continues to be subject to the FACTA "Red Flag Rules" requiring given its ongoing role in processing customer credit transactions.

admitted in its SEC filings that it had such “a program in place to detect and respond to data security incidents.” As set forth herein, Target did not, in fact, implement or adhere to an Identity Theft Protection Program that complied with federal law.

38. In particular, the Red Flag Rules regulations required that Target's data security program be regularly updated to account for developments in security threats and changes in Target's business. As the Federal Trade Commission ("FTC") explains, the plan should be updated to reflect Target's "experience with identity theft; changes in how identity thieves operate; new methods to detect, prevent, and mitigate identity theft; changes in the accounts you offer; and changes in your business, like mergers, acquisitions, alliances, joint ventures, and arrangements with service providers."

39. In addition, the Red Flag Rules required that the written Identity Theft Protection Program reflect the sophistication and size of the data security risk, and that it be sufficiently robust to account for the specific level of risk to which Target's customers' financial and personal data were exposed. Further, those regulations also required Target to modify its Identity Theft Protection Program to respond to any evolving threats to Target's data security, to tailor the plan to address any threats identified, and to ensure the plan was properly funded and staffed.

40. Moreover, as noted above, Minnesota's legislature enacted one of the strongest consumer data protection statutes in the country, which specifically codified some of the most pertinent provisions of the PCI DSS. That legislation, which was passed in the wake of the Gonzalez hacking scandal, was intended to address the very security deficiencies that led to the Target Data Breach at issue here. In particular, that law, the Plastic Card Security Act, imposes strict liability on merchants who "retain the card security code data, the PIN verification code number, or the full

contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction." Minn. Stat. § 325E.64. As explained by a representative from the Minnesota Credit Union Network, the Plastic Card Security Act was intended "to create an incentive [for retailers] to do the right thing and create consequences to prevent breaches from happening in the first place."

C. WARNING SIGNS: REPEATED BREACHES FROM 2007 TO 2012 PUT TARGET ON NOTICE THAT ITS POS SYSTEMS WERE VULNERABLE.

41. As early as 2007, Dr. Neal Krawetz of Hacker Factor Solutions published a white paper entitled "Point-of-Sale Vulnerabilities" (the "White Paper"). According to the White Paper, POS systems "provide virtually no security" and few POS systems "implement best practices for handling sensitive information, such as the Visa standards for credit card management."⁶

42. The White Paper also provided detailed descriptions of a typical POS system and its components, and described how those components' vulnerabilities could result in the compromise of millions of payment card accounts. Using Target, specifically, as an example, the White Paper prophesied the potential ramifications of a data breach in the Target POS system, accurately predicting that as many as 58 million payment card accounts could be breached if Target's POS system were compromised. As Dr. Krawetz observed:

Point-of-sale terminals and branch servers store credit card information in ways that are no longer secure enough. These vulnerabilities are not limited to any single POS vendor; they pose a fundamental hole in the entire POS market. It seems that nearly every POS provider is vulnerable, ... Similarly, these vulnerabilities impact all retailers that use these systems, including (but not limited to) OfficeMax, BestBuy, Circuit City, Target, Wal-Mart, REI, Staples, Nordstrom, and Petco. The amount of vulnerability varies between retailers and their implementations. But in general, if a credit card is not required to return a product, or the product can be returned at any

⁶ See <http://www.hackerfactor.com/papers/cc-pos-20.pdf>.

store, then the retailer likely has a serious vulnerability.⁷

43. Target got a copy of Dr. Krawetz's White Paper. On or about August 7, 2007, a Target employee responsible for Target's POS system acknowledged receipt of the White Paper and requested permission to provide it to other Target employees. The Target employee described Dr. Krawetz's suggestions as "good ideas."

44. Thereafter, at least 17 copies of the White Paper were downloaded to a domain owned by Target, the most recent download occurring in May 2013. Target personnel used the search term "POS vulnerability" to locate and download the White Paper. As is now apparent, Target did not heed the White Paper or implement its suggestions.

45. Ironically, Target had an opportunity to become an industry leader in data security during the early 2000s, when it explored a collaboration with Visa to promote the use of technologically advanced "chip cards" in Target stores. However, Target executives responsible for store operations and merchandising allegedly killed the chip card program because the technology slowed checkout speeds and did not offer Target sufficient marketing benefits. Checkout speed and marketing benefits were (and continue to be) more important to Target than the security of its customers' sensitive Payment Card information and PII.

46. Following Target's earlier decision to abandon security-enhancing "chip-card" technology, Target's POS security systems were repeatedly infiltrated by hackers, making clear the vulnerabilities in Target's systems. Since 2007, Target has suffered at least *four* other major POS system data breaches—one of which included a "massive" breach involving PII and sensitive payment card information.

⁷ See *Id* at 10.

47. In 2007, a computer hacker named Albert Gonzalez stole and resold more than 170 million card and ATM numbers from numerous retailers, including Target.⁸ He was able to obtain this information by pointing at Target's vulnerable POS systems. Target attempted to conceal the fact that it had been subject to the Gonzalez attack, and only later disclosed that its customers' information had been compromised after a blogger reported that Target had been an unnamed retailer described in an indictment against Gonzalez filed by law enforcement.

48. Following the Gonzalez scandal, data security experts warned that yet another potential data breach of Target's POS system was likely, and they provided information on how to prevent such a breach. Experts also warned that failure to implement preventative measures could result in an even larger data breach.

49. Predictably, in May 2010, hackers again exploited weaknesses in Target's POS systems. As reported by the online retailer security newsletter *FierceRetailIT*, in that instance, Target had somehow "overlooked security holes" in its POS systems that enabled customers to use funds from other shoppers' gift cards. The security expert who identified these "holes"—which included printing the full account number ("PAN" or "Primary Account Number") in the gift card's barcode—described them as fundamental security failures. According to the expert, "You never use the PAN on the handset. Never, never."

50. Third, in November 2010, Target was forced to issue a chain-wide software repair to resolve a coupon-scanning problem whereby consumers were given a small fraction of the promised discount. That error was reportedly the result of improperly functioning custom fraud-prevention coding in Target's POS systems. According to a report, the problem persisted for months before

⁸ See *United States v. Gonzalez*, Case Nos. 08-cr-10223-PBS (D. Mass. 2008) and 09-cv-10382 (D. Mass. 2009).

Target's IT department became aware of the issue, and Target was eventually required to completely shut down its POS systems in order to manually review coupons.

51. Fourth, on April 5, 2011, Target informed its "customers that their names and email addresses had been exposed in a massive online data breach" when a computer hacker penetrated the customer email databases in which Target retained customers' personal information.

52. All of these breaches were precursors to the latest Target Data Breach and demonstrate that, for years, Target has known that its POS systems are a focus of attack by thieves and hackers, but has systematically neglected to appropriately test and upgrade them. For years, Target has improperly failed to safeguard its customers' sensitive information.

53. Worse yet, Target failed to take reasonable measures to protect customer data even after it was specifically warned about the very type of cyber-attacks that eventually occurred in the months leading up to the Target Data Breach. For example, Visa issued at least two warnings last year—one in April 2013 and another in August 2013—alerting Target to attacks using malware known as a RAM scraper, or memory parsing software, that enables cyber criminals to grab encrypted data by capturing it when it travels through the live memory of a computer.

54. Visa warned Target that "[s]ince January 2013, Visa has seen an increase in network intrusions involving retail merchants," explaining that hackers would "install memory parser malware on the Windows based cash register system in each lane or on Back-of-the-House (BOH) servers to extract full magnetic stripe data." According to the warning, Visa was specifically aware of malware affecting the type of operating systems that Target used.

55. To guard against this threat, the Visa warnings instructed Target to, among other things, review its "firewall configuration and ensure only allowed ports, services and IP addresses are

communicating with your network"; "segregate the payment processing network from other non-payment processing networks"; "implement hardware-based point-to-point encryption"; "perform periodic scans on systems to identify storage of cardholder data and secure delete the data"; and "assign strong passwords to your security solution to prevent application modification." Target did not take the measures Visa instructed it to take.

D. BLACK FRIDAY 2013: THE TARGET DATA BREACH

i. Hackers infiltrate Target's POS systems and steal payment information.

56. The Target Data Breach began on November 27, 2013, as shoppers prepared to swarm Target's 1,800 stores looking for Black Friday deals. On or about that date, hackers gained access to Target's POS system within its internal computer network of systems through malicious computer code delivered via Fazio Mechanical Services, Inc., a Pittsburgh based refrigeration contractor, that Target had authorized to link remotely with Target's internal computer network of systems.

57. Although Target has been slow to disclose how its POS system was compromised, the WALL STREET JOURNAL reported:

In this case, malicious software, or malware, made its way onto Target's point-of-sale terminals -- the red credit-card swiping machines in checkout aisles -- according to people familiar with the breach investigation.⁹

58. Experts believe the injected malware was software known as Reedum (also known as Kaptoxa, a Russian slang word for potato), which is a variant of the BlackPOS malware specifically developed to attack POS systems. The Reedum malware works like a Trojan horse by hiding its malicious nature and compromising the target's POS system from the inside. Once it had been

⁹ See Sara Germano, Target Faces Backlash After 20-Day Security Breach: Retailer Says 40 Million Accounts May Have Been Affected Between Nov. 27 and Dec. 15, THE WALL STREET JOURNAL, Dec. 19, 2013.

injected into Target's POS system, the software sought out and monitored payment programs for Track Data on the Payment Cards' magnetic stripes, which, during the authorization process, was unencrypted and stored in the POS memory. Reedum then "scraped" the data and stashed it inside a hijacked Target server until the prime business hours of 10 a.m. to 5 p.m., allowing movement of the data to blend in with normal traffic.

59. Reedum transmitted its first payload of stolen payment card information to a hijacked internal Target network server on December 2, 2013. The hackers later harvested "scraped" stolen payment card information from the Target server by sending it over the Internet to a computer in Russia. They repeated this process numerous times over the next two weeks.

60. The stolen data was sufficient to permit the hackers to create fake credit cards and make fraudulent purchases or, in the case of debit cards, to withdraw money from victims' bank accounts.

61. Within days, the Secret Service (which is charged with protecting the country's financial infrastructure and payment systems, among other duties) noticed a flood of new stolen payment cards entering the market in alarming amounts of quarter-million or half-million batches. The Secret Service was able to associate these cards with Target-related uses and, accordingly contacted Target about the fraudulent activity several days prior to December 15, 2013. In response, Target commenced an internal investigation.

62. On December 19, 2013—four days after confirming internally that the Data Breach had occurred—Target announced to the world that hackers had injected malware into its POS system within its internal network and stolen sensitive Track Data contained on the magnetic stripes of 40 million payment cards, including customer names, credit or debit card numbers, expiration

dates, CVV codes, and PIN numbers (*i.e.*, "Track Data"), thereby giving fraudsters the data necessary to create fake credit and debit cards. Target publicly admitted the compromise of its payment card data and acknowledged that "guests who made credit or debit card purchases in [Target] U.S. Stores from Nov. 27 to Dec. 15, 2013" were impacted because "customer name, credit or debit card number, and the card's expiration date and CVV" had been stolen.

63. Target initially stated that PIN numbers pertaining to the stolen debit cards had not been stolen. Indeed, recognizing that the Data Breach threatened Target's sales during the peak holiday season, Target lured customers back into its stores by reassuring the public that the breach was minimal, contained, and "swiftly resolved." In addition, Target claimed that it had "no indication that debit card PINs were impacted." Indeed, Target claimed that it was "confident that PIN numbers were safe and secure" and that thieves could not just "visit an ATM with a fraudulent card and withdraw cash." Target even enticed customers back to its stores by offering a 10% discount during the remaining holiday shopping days, with Target CEO Gregg Steinhafel explaining that the discount was in the "spirit" of "we're in this together."

64. On December 27, 2013, however, Target finally admitted that hackers had also stolen PIN numbers during the Data Breach. But by then, the holiday shopping season was over.

65. On January 10, 2014, Target revealed for the first time that PII of an additional 70 million individuals had also been stolen in the Target Data Breach. The stolen PII includes customer names, mailing addresses, phone numbers and email addresses.

ii. Identity Thieves Begin Selling And Using The Stolen Payment Card Information.

66. The compromised Payment Cards consisted of cards used by shoppers who had visited Target stores between November 27, 2013, and December 15, 2013. On information and

belief, Visa, MasterCard, American Express and Discover-branded Payment Cards, as well as Target's REDcard private label Payment Cards, were affected. Krebs On Security, a closely-watched security blog that broke the public news of the Target Data Breach on December 18, 2013, reported that the Data Breach involved nearly every Target store in the United States.¹⁰

67. Even before Target finally elected to disclose the Data Breach to the public, the payment card processors were detecting a surge in fraudulent transactions that involved Payment Cards used at Target. The New York Times reported that as early as December 11, 2013, fraud analysts had detected "a ten to twentyfold increase in the number of high-value stolen cards on black market websites, from nearly every bank and credit union."¹¹

68. KrebsOnSecurity.com has reported that Payment Card information stolen and compromised in the Target Data Breach has flooded underground black markets and is being sold in batches of one million cards priced from \$20 to more than \$100 per card. Some financial institutions have reportedly purchased large blocks of their own Payment Card accounts from illicit online "card shops" in an effort to mitigate their losses.

69. One stolen payment card shop is well known for selling "dumps" of stolen Track Data collected from stolen payment cards. The stolen Track Data allows thieves to clone credit cards to make fraudulent purchases in stores and debit cards to withdraw cash from unsuspecting victims' bank accounts via ATMs.

70. Indeed, shortly after the Target Data Breach began, one card shop proprietor nicknamed "Rescator," who also is a key figure on "Lampeduza," a Russian-language cybercrime

¹⁰ Target claims its online business, Target.com, was not impacted. Time will tell.

¹¹ See Elizabeth A. Harris, Target Breach Affected Up to 110 Million Customers, N.Y. TIMES, Jan. 10, 2014.

forum, began advertising a new base of one million Payment Cards, dubbed "Tortuga."¹² Tortuga is a near anagram for Target.

71. KrebsOnSecurity.com also reported that it had been asked by a small issuer bank to help recover (through online purchase) the bank's credit card accounts compromised by the Target Data Breach. The first step was to determine if the bank's cards were, in fact, being offered for sale via the illicit card shop's website—described as "remarkably efficient and customer friendly." Like other card shops, this store allows customers to search for available Payment Cards using a number of parameters, including the BIN (a bank's unique number, which is the first six digits of a payment card), type of payment card (*e.g.*, MasterCard, Visa, etc.), expiration date, track type, country and/or the name of the financial institution that issued the card. Payment Cards stolen and compromised in the Target Data Breach were identified in the store as a mix of MasterCard dumps ranging in price from \$26.60 to \$44.80 apiece. As an additional service, the card shop also provides purchasers with the ZIP code and city location of the Target store from which the payment card information was stolen. *Id.* This information is valuable to fraudsters because they will make same-state purchases, thereby avoiding any knee-jerk fraud defenses a financial institution might use to block out-of-state transactions from a known compromised payment card. *Id.*

72. The issuing bank ran fraud and common POS analyses on each of the dumps it purchased and confirmed that all of the stolen and repurchased Payment Cards had been used to make purchases at Target stores between November 29, 2013 and December 15, 2013. Some Payment Cards had already been tagged "confirmed fraud," while others were only recently issued and had only been used at Target. KrebsOnSecurity.com and the bank also discovered that a

¹² See *Cards Stolen in Target Breach Flood Underground Markets*, KREBS ON SECURITY, Dec. 20, 2013, <https://krebsonsecurity.com/2013/12/whos-selling-credit-cards-from-target/>.

number of the stolen and repurchased Payment Cards were flagged for fraud after the Target Data Breach because they were used to make unauthorized purchases at big box retailers like Target.

E. THE DATA BREACH OCCURRED BECAUSE TARGET DID NOT MEET INDUSTRY STANDARDS.

i. Target does not prioritize data safety.

73. At the time of the Data Breach, Target was not in compliance with the Plastic Card Security Act, the PCI DSS, the Card Operating Regulations, or the Red Flag Rules.

74. Ken Stasiak, CEO of a PCI forensic investigator called SecureState has explained that, "[f]or a hacker to be able to infiltrate Target's network and access the POS application, several PCI-DSS and PA-DSS [Payment Application Data Security Standard] controls must not have been implemented effectively. Thus, Target was not compliant during the time of the breach." Indeed, as Stasiak explained, ensuring compliance with PCI DSS standards would have prevented the very sort of Data Breach that occurred: "We handle these investigations for the payment card brands, and in all of the investigations we performed, the merchant was not compliant to PCI-DSS controls during a breach."

75. Target failed to implement and maintain the necessary safeguards because doing so cut into profits. Indeed, Target's IT department, called Target Technology Services, chooses cost-effective but not actually effective technology to deploy across Target's stores. As explained by Target's Director of Infrastructure Engineering, Brad Thompson ("Thompson"), in a study analyzing Target's systems, the Target's IT systems are "a cost center, and so [it is] always looking to drive down costs where possible." In the same case study, Target's Senior Group Manager of Server Technology and Enterprise Storage, Fritz DeBrine, said that "[t]o keep our management costs down, it's in our best interests to have a streamlined IT infrastructure at each store."

76. For instance, when Target Technology Services team members are asked to deploy new software, application upgrades, or security updates, Target's management has required that they be done as quickly as possible so as to not interrupt shopping hours to ensure sales are not jeopardized. According to Thompson,

There are only a few hours at night when we can do deployments without disturbing scheduled processes, such as POS system maintenance The control room has to be up and running by 7 a.m. because we can't do anything that puts opening the doors at risk.

77. Further, Target has admitted that it retains customer data in connection with its credit and debit transactions in order to try to increase sales and for strategic marketing purposes, and that it keeps such data for 60-80 days. That fact was confirmed by John Deters, a Target engineering consultant who testified on behalf of Target in litigation alleging that Target violated provisions of the Fair and Accurate Credit Transaction Act [FACTA] by improperly printing credit and debit account information—including the full account number and card expiration date—on credit and debit transaction receipts. As Deters testified, "Target retain[s] the full account number" and "then store[s] that information regarding the transaction, including the account numbers... of the credit card or debit card and the expiration date and the cardholder's name, in its computer system."

78. PCI DSS and the Card Operating Regulations explicitly prohibited Target from retaining or recording specified customer information. For example, Target's agreement with MasterCard prohibited Target from recording PIN data provided by customers, even in encrypted form. As set forth in MasterCard's Security Rules and Procedures-Merchant Edition, dated January 29, 2010, "MasterCard prohibits the recording of PIN data and CVV data in any manner for any purpose."

ii. Target outsourced its data security obligations to Trustwave—which failed to bring Target's systems up to industry standards.

79. In order to keep its costs down, Target does not have its own IT team members working at its stores. Instead, Target contracts with a third-party IT services provider—Trustwave.

80. The PCI Security Standards Council specifically warns retailers that relying on third-party vendors to perform credit and debit transaction services poses special risks to merchants, and that "organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements."

81. Trustwave publicly claims that it is "a PCI-approved scanning vendor and Qualified Security Assessor (QSA)," and that it offers "a full breadth of services to help retailers comply with PCI DSS." In particular, Trustwave advertises itself as having "deep expertise in PCI Compliance."¹³ Trustwave acknowledges the stakes for its services on its website, where it correctly notes that "Cyber attackers are targeting retail businesses at an increasing rate because the sensitive data [retail businesses] process every day is highly valuable."¹⁴

82. Upon information and belief, Target retained Trustwave during the relevant period of time to protect and monitor Target's computer systems, and to bring Target's systems into compliance with PCI DSS and other industry standards for protecting customers' PII and sensitive payment card information. According to Trustwave, it has "performed more Payment Card Industry Data Security Standard (PCI DSS) Certifications than all other companies combined."

83. On information and belief, Trustwave scanned Target's computer systems on

¹³ See <https://www.trustwave.com/Solutions/By-Industry/Solutions-for-the-Retail-Industry/>.

¹⁴ *Id.*

September 20, 2013 and told Target that there were no vulnerabilities in Target's computer systems.

84. To the contrary, however, and as reported by the *The New York Times*, Target kept credit and debit card data on its servers for six full days before hackers transmitted the data to a separate webserver outside of Target's network. Because of these vulnerabilities in Target's security systems—either undetected or ignored by Trustwave—hackers were able to take 40 million Payment Card records, encrypted PINs, and 70 million records containing Target customer information over the course of two weeks.

85. Additionally, on information and belief, Trustwave also provided round-the-clock monitoring services to Target, which monitoring was intended to detect intrusions into Target's systems and compromises of PII or other sensitive data. In fact, however, the Data Breach continued for nearly three weeks on Trustwave's watch.

86. Trustwave failed to live up to its promises, or to meet industry standards. Trustwave's failings, in turn, allowed hackers to cause the Data Breach and to steal Target customers' PII and sensitive payment card information. In addition, Trustwave failed to timely discover and report the Data Breach to Target or the public.

F. THE TARGET DATA BREACH WAS PREVENTABLE AND NEVER SHOULD HAVE HAPPENED.

87. The Target Data Breach was preventable. Target knew, at least as early as 2007, that its data security policies, procedures, protocols, and hardware and software systems were insufficient, antiquated, and did not safeguard and protect sensitive consumer data from theft, yet did not correct the problems. Target should have taken the following steps, each of which likely would have prevented the Data Breach.

- i. Target should have implemented Dr. Krawetz' White Paper suggestions and

brought Target's internal computer network and POS system into compliance with PCI DSS and PCI PED.

- ii. Target should have instituted an effective Enterprise Risk Management ("ERM") system supported by the appropriate ERM software. With an effective ERM process, the risk of a data breach would have been documented and assessed in a way that would have provided transparency to Target senior management who, in turn, would have had the time and opportunity to take steps to prevent the Target Data Breach before it occurred. Even for an entity the size of Target, a fully developed ERM system would have cost Target substantially less than 3% of the estimated cost of the Target Data Breach.¹⁵ On information and belief, however, Target failed and refused to develop and implement an effective ERM system—much less, an ERM system of any kind.
- iii. Target should have installed the appropriate antivirus software in its POS system and across its entire internal network. Several readily available antivirus software programs such as AVG, Bitdefender and ThreatTrack would have detected and removed the malware used by the hackers. On information and belief, however, Target failed and refused to install appropriate antivirus software in its POS system and across its entire internal computer network.
- iv. Target should have set the policies on its local store computers in its POS system to disable the installation of malware such that its installation would have been

¹⁵ According to the Ponemon Institute, a data breach costs U.S. companies an average of \$188 per compromised customer record—which pegs the total estimated cost of the Data Breach to Target at over \$7.5 billion. *See 2013 Cost of a Data Breach Study*, United States, PONEMON INSTITUTE, June 13, 2013.

impossible. On information and belief, however, Target failed and refused to set the policies on its local store computers in its POS system to disable the installation of malware.

- v. Target should have implemented basic security measures related to authentication—specifically, two-factor authentication on its POS terminals for anyone attempting to remotely connect to them. On information and belief, however, Target failed and refused to implement these authentication-based basic security measures on its POS terminals.
- vi. Target should have properly monitored its POS system for signs of attack. On information and belief, however, Target failed and refused to properly monitor its POS system.
- vii. Target should have disconnected its POS systems from the Internet. There is no reason for POS terminals to be freely accessible via the Internet. At the very least, outbound access to the Internet by the POS system should have been blocked by a firewall, which would have prevented the hackers from uploading stolen payment card information to the Internet and Russia.

88. The key to effective data security is layered security, which Target did not have in place. Had layered data security been in place, the data thieves would first have had to determine how to deploy the malware, and then determine how to circumvent the antivirus software running on the POS terminals. Even if they could have accomplished these feats, which they could not, the malware would have been blocked by a firewall or network segmentation when trying to access the Internet. In other words, the Data Breach would not have happened if Target had actually followed

the industry standards and best practices as it claimed.

G. TARGET SAYS IT ACCEPTS FULL RESPONSIBILITY FOR THE DATA BREACH—BUT HAS NOT COMPENSATED CLASS MEMBERS.

89. In a January 13, 2014, interview with CNBC's Becky Quick, Gregg Steinhafel. (“Steinhafel”), Target's Chairman, CEO and President, stated

Yeah, zero liability is zero liability, which means Target is paying for any, any possible fraudulent activity on anybody's credit card... We're in the middle of this investigation. And we haven't got to the end of this investigation... But there's a process that plays out. And the issuing banks work with – networks and processors. And ultimately, we're responsible and we're accountable for this. There's no doubt. And, so, we will incur the losses associated with that.

90. Target has repeatedly pledged that no consumer will sustain any damages as a result of the Target Data Breach—mostly by pointing to its offer to provide affected customers with one free year of a single-bureau credit monitoring service called Experian ProtectMyID. According to Consumer Reports, however, Target “fumbled” when it offered this “second-rate credit-monitoring service.” At best, the ProtectMyID credit monitoring service is an indirect manner of tracking identity theft; it may reveal new credit accounts opened with the stolen information, but it does nothing to monitor unauthorized charges made to existing Payment Card accounts.¹⁶

91. Thus, although Target has made some gestures toward preventing fraud based on the stolen PII and sensitive payment card information, Target has not alleviated the need for Trustmark and other Class members to protect their (and Target's) customers by cancelling and reissuing the stolen and compromised Payment Cards, and to absorb the fraudulent charges being made with the compromised Payment Cards.

¹⁶ See *Consumer Reports Calls Target's Response to Data Breach Weak*, UPI, Feb. 6, 2014, http://www.upi.com/Business_News/2014/02/06/Consumer-Reports-calls-Targets-ersponse-to-data-breach-weak/UPI-69291391732657/print#ixzz2sf1Hce3T.

i. The damage done to the Banks and the other Class members is monumental.

92. After learning about the Target Data Breach, the Banks and other Class members took steps to limit their losses—including cancelling and reissuing compromised Payment Cards.

93. In fact, it has been estimated that the costs to banks and retailers caused by the Target Data Breach could eventually exceed \$18 billion. Frank Keating, President and CEO of the American Bankers Association, wrote in a January 16, 2014, letter to Congress that, "When a retailer like Target speaks of its customers having 'zero liability' from fraudulent transactions, it is because *our nation's banks* are providing that relief, not the retailer that suffered the breach."

94. According to the Consumer Bankers Association ("CBA"), to date, the Target Data Breach has cost its U.S. member banks over \$172 million just to re-issue the stolen Payment Cards.¹⁷ This figure does not include fraudulent purchases and unauthorized cash withdrawals the banks have also had to absorb. Specifically regarding the Target Data Breach, Richard Hunt, President and CEO of the CBA, opined:

When retailers say this data breach comes at no cost or liability to consumers they are right - because it is banks and card issuers who are on the hook often at little or no cost to retailers like Target. Retailers should recognize that the costs of data breaches snowball with time and should take responsibility when they are at fault.¹⁸

95. A recent analysis by global investment banking firm Jefferies suggests that payment card issuers could sustain upwards of \$1 billion of damages as a result of the Target Data Breach based on an estimated 4.8 million to 7.2 million stolen and compromised Payment Cards being used to make fraudulent purchases and unauthorized cash withdrawals. These costs fall on Trustmark and the other Class members, even though they had nothing to do with causing the Data Breach and

¹⁷ See <http://www.fnextra.com/news/fullstory.aspx?newsitemid=25702&topic=payments>.

¹⁸ *Id.*

could not have avoided it.

96. Indeed, after just one billing cycle, the Banks have already been forced to reissue nearly 1,000 cards, refund thousands of dollars in fraudulent purchases, and expend other sums in order to notify its customers of the Breach and the threat to their Payment Cards' data. Other Class members have had to reissue many more cards. The Banks and the other Class members will continue to incur significant damage as a result of the Target Data Breach, which affected more than 110 million customers—the majority of whom used cards issued by one of the Class members.

VII.
THE TARGET BREACH CAUSED SUBSTANTIAL DAMAGE TO THE CLASS

97. As a result of the Target Data Breach, the Banks and the other Class members were required to take reasonable measures to protect their customers and avoid fraud losses, including by cancelling the Payment Cards they had issued, reissuing new cards, and refunding fraud-related charges.

98. Indeed, as a result of the Target Data Breach, the Banks and the other Class members suffered losses for reimbursing fraudulent charges and reversing customer charges, notifying customers that their data had been compromised, and reissuing and mailing new cards to its customers.

99. These costs and expenses will likely increase as additional fraud alerts and charges are discovered and occur. Alphonse R. Pascual of Javelin Strategy & Research has said the stolen data would continue to be exploited by criminals in the months ahead, explaining that "We're expecting this to be a major contributor, if not the primary driver of card fraud for the next 12 months."

**VIII.
CAUSES OF ACTION**

**COUNT ONE
NEGLIGENCE (ALL DEFENDANTS)**

100. The Banks repeat and re-allege each and every allegation contained above as if fully set forth herein.

101. When Target came into possession of private, non-public, sensitive payment card information and PII belonging to the Banks' customers and the customers of the other Class members, Defendants incurred and maintained a continuing duty to exercise reasonable and due care to safeguard and protect that information from theft and loss.

102. It was reasonably foreseeable to Defendants that a failure to safeguard and protect sensitive payment card information and PII belonging to the Banks' customers and the customers of the other Class members would cause direct and immediate damage to the Banks, the other Class members and their customers. Target knew that a loss or theft of sensitive payment card information and PII would require the Banks and the other Class members to take steps to protect their customers' PII and payment card information, including without limitation incurring expenses to notify their customers of the data breach and reissuing payment cards.

103. Additionally, Defendants undertook a duty to safeguard and protect payment card information and PII from theft and loss when Target elected to comply with industry standards for the protection of PII and other sensitive data by, among other things, purporting to adopt and comply with the PCI DSS protocols, participating in the Visa and MasterCard Networks subject to the applicable Visa Operating Regulations and MasterCard Rules, and by representing to the public and all Target customers that it was purporting to meet these standards. Indeed, Target made these

public representations to induce potential customers to shop at Target and to rely on Target's payment processing systems as convenient, safe, and secure.

104. Defendants knew, or, with the reasonable exercise of care, should have known, of the risks inherent in retaining such information, and the importance of providing adequate security.

105. Because Defendants reasonably and actually foresaw that a data breach would cause damage to its customers and to the Banks and the other Class members' customers, they had a duty to implement the appropriate customer data security policies, protocols, and hardware and software systems—especially in its POS systems—to prevent and detect data breaches and the unauthorized appropriation of Trustmark's and the other Class members' customers' PII and Payment Cards' information.

106. Defendants failed to implement appropriate customer data security policies, protocols, and hardware and software systems throughout their facilities and especially on Target's POS systems.

107. For example, Target inappropriately gave one of its vendors access to Target's internal computer networks and POS systems without adequate security procedures and safeguards, with the result that data thieves were able to place malicious software or hardware on Target's computer systems and thereby obtain PII and payment card information to which the thieves never should have had access.

108. As a result of Defendants' breach of their duties to the Banks, the Banks' customers, the Class members, and the Class members' customers, among others, the Data Breach occurred and compromised millions of individuals' PII and sensitive payment card information.

109. Additionally, Defendants breached their duties to the Banks' customers and the

customers of the other Class members by failing to properly and timely notify those customers, the Banks, and the other Class members that their PII and payment card information had been compromised and stolen.

110. As a direct and foreseeable result of Defendants' failure to safeguard and protect PII and payment card information, and to notify Target's customers, the Banks, and the other Class members of the Data Breach, the Banks and the other Class members incurred damages consisting of the expenses required to notify their customers of the Data Breach, to cancel and reissue compromised Payment Cards, and to reimburse or otherwise absorb unauthorized charges made on the compromised Payment Cards. Absent Defendants' negligence, the Banks and the other Class members would not have incurred these damages.

111. Defendants' negligence directly and proximately caused the Banks and the other Class members to suffer the above-described damages.

COUNT TWO

VIOLATIONS OF MINN. STAT. § 325E.64 (THE "PLASTIC CARD ACT") (ALL DEFENDANTS)

112. The Banks repeat and re-allege each and every allegation contained above as if fully set forth herein.

113. At all relevant times, Minn. Stat. § 325E.64 (the "Plastic Card Act") prohibited Target from retaining the customer personal and financial data it obtained through its POS systems, specifically including PII and sensitive payment card information. Specifically, the subdivision 2 of the Plastic Card Act provides that:

No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit

transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

114. Defendants failed to comply with Subdivision 2 of the Plastic Card Act with respect to credit card transactions. For credit card transactions, Target's POS devices and systems retained the card security code, PIN verification code number, and the full contents of payment card magnetic stripe data subsequent to authorization of the legitimate transactions being made by Target customers. Indeed, Target's POS devices and systems retained all of that information until a later time when those devices and systems sent PII and sensitive payment card information to unauthorized persons.

115. Defendants also failed to comply with Subdivision 2 of the Plastic Card Act with respect to debit card transactions. For debit card transactions, Target's POS devices and systems retained the card security code, PIN verification code number, and the full contents of payment card magnetic stripe data subsequent to 48 hours after authorization of the transaction. As with credit card transactions, Target's POS devices and systems retained all of that information until a later time when those devices and systems sent PII and sensitive payment card information to unauthorized persons.

116. Because Defendants breached the Plastic Card Act, Defendants have strict liability for the Data Breach that occurred here pursuant to Subdivision 3, which provides:

Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders.

117. Target maintains its headquarters and principal place of business in Minnesota and accepts access devices at its approximately 75 stores in Minnesota, as well as in over a thousand other stores in the United States, including stores in Illinois.

118. Trustwave maintains its principal place of business in Chicago, Illinois and provided IT services to all of Target's retail stores throughout the United States.

119. The Banks and other members of the Class took reasonable actions to protect themselves and the information of their cardholders and to continue to provide services to their cardholders, and incurred significant costs in doing so. The costs borne by the Banks and members of the Class include costs associated with:

- i. canceling and reissuing access devices affected by the Data Breach;
- ii. closing deposits, transactions, share drafts, and other accounts affected by the Data Breach and taking actions to stop payments and block transactions with respect to those accounts;
- iii. opening and reopening deposit, transaction, share draft and other accounts affected by the Data Breach;
- iv. refunding and crediting cardholders to cover the costs of unauthorized transactions relating to the Data Breach;
- v. notifying cardholders affected by the Data Breach; and
- vi. paying damages to cardholders injured by the Data Breach.

120. Accordingly, Defendants are strictly liable to the Banks and the other members of the Class for these above-described costs due to Target's violation of Minn. Stat. § 325E.64, as set forth above.

COUNT THREE

VIOLATIONS OF MINN. STAT. § 325F.69 (DECEPTIVE PRACTICES) (ALL DEFENDANTS)

121. The Banks repeat and re-allege each and every allegation contained above as if fully set forth herein.

122. Defendants are corporations engaged in trade or commerce in the State of Minnesota, and are a "person" within the meaning of Minn. Stat. § 325F.68, Subd. 3, and therefore also within the meaning of Minn. Stat. § 325F.69.

123. Defendants' false representations and omissions regarding its compliance with the Plastic Card Security Act, PCI DSS, the FACTA "red flag" safeguards, and the Card Operating Regulations—as well as its actions in retaining, failing to safeguard, and allowing access to confidential customer data—constitute deceptive acts and unfair trade practices within the meaning of Minn. Stat. § 325F.69, Subd. 1.

124. Defendants' conduct in connection with its representations and omissions concealing their failures and misconduct regarding the confidential debit and credit cardholders' information constitute deceptive acts and unfair trade practices, having a direct and substantial effect in Minnesota and throughout the United States causing substantial damages to the Banks and to the other Class members.

125. Defendants' misrepresentations and omissions were made to and directed at the public at large, and the misconduct as alleged herein has affected tens of millions of consumers, as well as thousands of financial institutions that comprise the Class.

126. The Banks and the other Class members relied on Defendants' unfair and deceptive acts and practices as described above.

127. The Banks and the other Class members suffered damages as a result.

COUNT FOUR
VIOLATIONS OF MINN. STAT. § 325F.67 (FALSE ADVERTISING) (TARGET)

128. The Banks repeat and re-allege each and every allegation contained above as if fully set forth herein.

129. Target is a corporation engaged in trade or commerce in the State of Minnesota, and is a "person" within the meaning of Minn. Stat. § 325F.68, Subd. 3, and therefore also within the meaning of Minn. Stat. § 325F.67.

130. Target made the false representations and omissions regarding its compliance with the Plastic Card Security Act, PCI DSS, the FACTA "red flag" safeguards, and the Card Operating Regulations—as well as its actions in retaining, failing to safeguard, and allowing access to confidential customer data—with intent to sell merchandise and services, including without limitation the convenience of its payment processing services, to the public with intent to increase the consumption thereof.

131. Target also made these false representations and omissions in materials that it published, disseminated, circulated, and placed before the public by way of written and electronically-promulgated statements about Target's handling, safeguarding, and protection of customers' PII and sensitive payment card information.

132. Target's false representations contained material assertions, representations, and statements, of fact that were untrue, deceptive, and misleading.

133. Accordingly Target has created a public nuisance by its false representations and deceptive acts, and should be enjoined from making such statements and doing such acts.

COUNT FIVE
INJUNCTIVE RELIEF (MINN. STAT. §§ 325D.45 AND 325F.70) (TARGET)

134. The Banks repeat and re-allege each and every allegation contained above as if fully set forth herein.

135. In the aftermath of the Data Breach, Target continues to make public statements that it adequately protects PII and sensitive payment card information. On March 14, 2014, Target publicly released its Form 10-K annual report for 2013. In its 2013 annual report, Target publicly stated that its "network was determined to be compliant" with "applicable payment card industry standards" by "an independent third-party assessor in the fall of 2013." Also in the 2013 annual report, Target declined to commit to a substantial upgrade of its POS or other card payment processing systems, saying that "we are unable to estimate such investments [in upgraded information technology systems] because the nature and scope has not yet been determined," and forecasting that "[w]e do not expect such amounts to be material to any fiscal period."

136. Target's statements about the adequacy of protection it affords to customers' PII and sensitive payment card information are empirically false, as demonstrated by the Data Breach. The public will not be sufficiently protected by Target's continued misrepresentations and any voluntary improvements it may or may not elect to make to its information technology systems and POS devices.

137. The Banks, the Banks' customers, the other Class members, and the other Class members' customers have been damaged, and are likely to continue damaged, by Target's deceptive trade practices, as described by Minn. Stat. § 325D.45, Subd. 1.

138. Additionally, for the reasons discussed above, Target has engaged in practices that violate, and are made enjoined by, Minn. Stat. § 325F.69. Accordingly, the Minnesota attorney

general or any private attorney general acting in accordance with Minn. Stat. § 8.31, Subd. 3a may seek an injunction prohibiting further violations.

139. The Banks and the Class members seek an injunction for the benefit of the public at large.

140. In particular, but without limitation, this Court should, for a time period deemed appropriate by this Court but not less than two years, order and enjoin Target:

- i. from representing in any publicly published advertisement, circular, signage, electronic statement, or other public document that Target's POS devices and information technology systems, generally, are in compliance with PCI DSS, the FACTA "red flag" safeguards, or any other industry or government-specified standard or purported standard for the protection and maintenance of PII and sensitive payment card information except to the extent and at such a time that an independent special master appointed by this Court confirms to the Court's satisfaction that Target is, in fact, complying with such standard; and
- ii. requiring Target to bring its POS devices and information technology systems, generally, into compliance with all industry and government-specified standards for the protection and maintenance of PII and sensitive payment card information, and to use best practices for the protection and maintenance of that information, as supervised by an independent special master appointed by this Court.

COUNT SIX
UNJUST ENRICHMENT & GOOD FAITH RELIANCE (TARGET)

141. The Banks repeat and re-allege each and every allegation contained above as if fully

set forth herein.

142. Target has been unjustly enriched by its failure to protect PII and sensitive payment card information from theft, loss, and other forms of compromise, and by its false representations to the Banks, the Banks' customers, the other Class members, and the other Class members' customers. For example and without limitation, Target has benefitted from receiving:

- i. revenue from payment card transactions made using the card payment information lost or compromised during the Data Breach;
- ii. the saved costs of not implementing proper customer data security policies, procedures, protocols, and hardware and software systems in Target's POS systems; and
- iii. increased sales resulting from customers' reliance on Target's false assurances and representations that it had taken certain appropriate and industry-standard steps to protect customer PII and sensitive payment card information from theft and loss.

143. The Banks, the Banks' customers, the other Class members, and the other Class members' customers may recover their damages, described above, based on their good faith reliance upon Target's false representations and assurances because it would be inequitable for Target to benefit at their expense while failing to disclose the truth.

144. Therefore, Target should be compelled to refund or disgorge all wrongfully collected funds pursuant to the equitable doctrines of unjust enrichment and good faith reliance.

COUNT SEVEN
NEGLIGENCE PER SE (ALL DEFENDANTS)

145. The Banks repeat and re-allege each and every allegation contained above as if fully set forth herein.

146. At all relevant times, Defendants were required to comply with, *inter alia*, the applicable industry standards requiring Defendants to implement internal systems controls to prevent, detect and respond to system intrusions, and to securely handle and transfer sensitive financial data. These standards include, without limitation, the PCI DSS standard, the FACTA "red flag" safeguard standards, and the Card Operating Regulations.

147. Defendants were also required to comply with Minnesota's Plastic Card Act.

148. These regulations and industry security standards establish the minimal duty of care owed by Defendants to the Banks and the other Class members.

149. Defendants failed to comply with Minn. Stat. § 325E.64, the PCI DSS, and the FTC's Red Flag Rules. As set forth above, among other things, Target's internal systems retained card security code data, the PIN verification code number, and/or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, 48 hours after the authorization of the transaction in violation of Minn. Stat. § 325E.64.

150. Upon information and belief, had Defendants actually been in PCI DSS compliance during the relevant time period, the Target Data Breach would not have occurred.

151. Upon information and belief, had Defendants actually been in compliance with the Red Flag Rules under 16 C.F.R. Part 681 during the relevant time period, the Target Data Breach would not have occurred.

152. Defendants' violations of the Card Operating Regulations and other and industry

security standards constitute negligence per se and directly and proximately caused the Banks and the other Class members to suffer substantial damages.

153. The Banks and the other Class members were within the class of persons intended to be protected by these regulations and industry security standards, Minn. Stat. § 325E.64, and the Red Flag Rules. The injuries suffered by the Banks and the Class members were of the type intended to be prevented by these regulations and industry security standards.

COUNT EIGHT
NEGLIGENT MISREPRESENTATION (TARGET)

154. The Banks repeat and re-allege each and every allegation contained above as if fully set forth herein.

155. Target falsely represented to the Banks, the Banks' customers, the other Class members, the other Class members' customers, and the public at large that Target would safeguard and protect PII and sensitive payment card information that they provided to Target. Among other representations, Target assured the public that:

- i. Target adheres to "industry standard methods to protect [sensitive customer] information;" and
- ii. "When [Target] collect[s] or transmit[s] sensitive information such as a credit or debit card number, we use industry standard methods to protect that information;"

156. Target knew or reasonably should have known that these representations were false. Among other reasons, Target had actual and specific knowledge that its data security systems were inadequate to meet industry standard methods—*e.g.*, the PCI-DSS standards and FACTA "red flag"

safeguards—based on, among other things, the 2007 Gonzalez hacking scandal, the Krawetz White Paper, and Target's own evaluation and review of its systems.

157. Target made these representations with the intent that the Banks, the Banks' customers, the other Class members, the other Class members' customers, and the public at large rely on them. Indeed, Target made these representations intending that the recipients of those representations would decide to shop at Target stores instead of at competitors' stores, and would feel assured that making credit and debit card transactions at Target stores was safe.

158. The Banks, the Banks' customers, the other Class members, and the other Class members' customers, had no reason to doubt Target's false representations and justifiably relied on them.

159. Target's false representations caused the Banks, the Banks' customers, the other Class members, and the other Class members' customers to shop at Target with their credit or debit cards or, in the alternative, to select credit or debit cards as methods of payment instead of another form of payment such as cash, and thereby subject their PII and sensitive payment card information to theft and fraud following the Data Breach.

160. As a result, Target's false representations directly and proximately caused damage to the Banks and the other Class members to suffer the above-described damages.

IX. PRAYER FOR RELIEF

WHEREFORE, Trustmark National Bank and Green Bank, N.A. pray for judgment as follows:

- i. determining that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure, appointing the Banks as a representative of the Class and their counsel

- as Lead Counsel for the Class pursuant to Fed. R. Civ. P. 23(g);
- ii. awarding compensatory damages in favor of the Banks and other Class members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;
 - iii. awarding statutory damages in favor of the Banks and other Class members against Defendants;
 - iv. awarding the Banks and the Class their reasonable costs and expenses incurred in this action, including expert fees, the costs of investigation and reasonable attorney's fees pursuant to Minn. Stat. § 8.31, Subd. 3a or any applicable provision;
 - v. issuing an order and injunction substantially in the form described in Count Eight, above; and
 - vi. awarding such equitable, injunctive, or other relief as the Court deems just and proper.

X.
JURY DEMAND

Plaintiffs Trustmark National Bank and Green Bank, N.A. demand a trial by jury.

Dated: March 24, 2014.

Respectfully submitted,

MORGAN & MORGAN

By: /s/ Panagiotis V. Albanis
Panagiotis V. Albanis
Illinois State Bar No. 6277031
palbanis@forthepeople.com

12800 University Drive, Suite 600
Fort Meyers, Florida 33907
(239) 432-6605 (telephone)
(239) 433-6836 (facsimile)

STECKLER LAW, LLP

Bruce W. Steckler (*Pro Hac Vice* Admission Pending)
Texas Bar No. 00785039
bruce@stecklerlaw.com
12720 Hillcrest Road, Suite 1045
Dallas, Texas 75230
(972) 387-4040 (telephone)
(972) 387-4041 (facsimile)

KANE RUSSELL COLEMAN & LOGAN PC

Kenneth C. Johnston (*Pro Hac Vice* Admission Pending)

Texas State Bar No. 00792608

kjohnston@krcl.com

Robert W. Gifford (*Pro Hac Vice* Admission Pending)

New York Bar No. 4046231

rgifford@krcl.com

David M. Clem (*Pro Hac Vice* Admission Pending)

Texas State Bar No. 24050428

dclem@krcl.com

3700 Thanksgiving Tower

1601 Elm Street

Dallas, Texas 75201

(214) 777-4200 (telephone)

(214) 777-4299 (facsimile)

**ATTORNEYS FOR PLAINTIFFS
TRUSTMARK NATIONAL BANK
and GREEN BANK, N.A.**