IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

COMMUNITYBANK OF TEXAS, N.A., and FNBT.COM, INC., individually and on behalf of all others similarly situated, Plaintiffs, v. TARGET CORPORATION, Defendant.	CASE NO: CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiffs CommunityBank of Texas, N.A. ("CommunityBank"), and FNBT.com, Inc. ("FNBT"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters, by and through counsel, bring this Class Action Complaint against Target Corporation ("Target" or the "Defendant").

INTRODUCTION

1. Between November 27, 2013 and December 15, 2013, the credit card and debit card information (cardholder names, card numbers, expiration dates, security validation codes, and encrypted debit PINs) of approximately 40 million Target customers and the personal information (names, mailing addresses, telephone numbers, and email addresses) of approximately 70 million Target customers were stolen by hackers (the "Security Breach").

2. The Security Breach was the direct and foreseeable result of Target's failure to implement and maintain reasonable and industry-standard security measures to protect its customers' credit card, debit card, and personal information.

3. This nation's financial institutions, including CommunityBank and FNBT, have been left on the hook for tens, if not hundreds, of millions of dollars as a result of Target's failure to

implement reasonable and industry-standard measures, Target's otherwise willful and negligent conduct to protect its customers' credit card and debit card information, and the resulting Security Breach. Specifically, CommunityBank, FNBT, and other financial institutions have suffered losses resulting from and relating to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest for transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer concerns and anxiety; and f) lost customers.

4. Target has publicly acknowledged that it is responsible for the Security Breach and all damages stemming from it, for both its customers and their financial institutions.

JURISDICTION AND VENUE

5. This Court has jurisdiction under 28 U.S.C. §1332(d) because: (a) this matter was brought as a class action under Fed. R. Civ. P. 23; (b) the class (as defined below) has more than 100 members; (c) the amount at issue exceeds $5,000,000, exclusive of interest and costs; and (d) at least one proposed Class member is a citizen of a state different from Target.

6. This Court has personal jurisdiction over Target because the Target is headquartered and incorporated in the State of Minnesota.

7. Venue is proper in this Court under 28 U.S.C. § 1391(b)(1), (b)(2) & (c)(2), because, inter alia, Target conducts substantial business in this district and is subject to personal jurisdiction in this district. Finally, venue is proper in this district because a substantial part of the events giving rise to the claims at issue occurred in this district and emanated from decisions made in this district.

PARTIES

8. Plaintiff CommunityBank of Texas, N.A, is a Texas bank headquartered at 5999 Delaware Street, Beaumont, Texas. CommunityBank has 35 branch locations located throughout Southeast Texas.

9. Plaintiff FNBT.com, Inc., is a Florida bank headquartered at 29 North Elgin Parkway, Fort Walton Beach, Florida. FNBT has offices located throughout the State of Florida.

10. Defendant Target Corporation is a Minnesota corporation with its principal place of business located in Minneapolis, Minnesota. Target conducts business at its brick-and-mortar stores throughout the United States, excluding Vermont.

FACTUAL ALLEGATIONS

I. The Target Security Breach

11. Target advertises and sells merchandise directly to millions of consumers through its retail stores in the United States. In 2013, Target reported annual sales of $73.3 billion.

12. Target's U.S. stores use Point-of-Sale computer systems ("POS Systems"), which store credit card and debit card information. When a customer makes a purchase at a Target retail store using a credit card or debit card, Target collects information relating to that card, including the card holder's name, account number, expiration date, card verification number, and personal identification number ("PIN") for ATM/debit cards. Target then stores this information in its POS system and transmits this information to a third party for completion of the payment.

13. Target also collects and stores customer names, mailing addresses, phone numbers and email addresses on its network.

14. Between at least November 27, 2013 and December 15, 2013, hackers infiltrated Target's POS Systems and network, and stole the credit card and debit card information of approximately 40 million Target customers. The stolen credit card and debit card information

included cardholder names, credit card and debit card numbers, card expiration dates, three-digit security codes, and encrypted debit card PIN numbers.

15. On January 10, 2014, Target also announced that, in addition to the credit card and debit card information of approximately 40 million customers, the personal information—including names, mailing addresses, phone numbers and email addresses—of approximately 70 million individuals was also stolen as part of the Security Breach.

16. Upon information and belief, the hackers infiltrated Target's POS Systems and computer network by installing malware that intercepted and copied credit card and debit card "track" data, including cardholder names, card numbers, expiration dates, security codes, and encrypted debit card PINs. Subsequently thereto, the malware sent the card "track" data back to the hackers.

17. Upon information and belief, the hackers also infiltrated other aspects of Target's computer network, allowing them to steal the personal information of approximately 70 million individuals.

II. Target Failed to Maintain Reasonable and Industry-Standard Security Measures

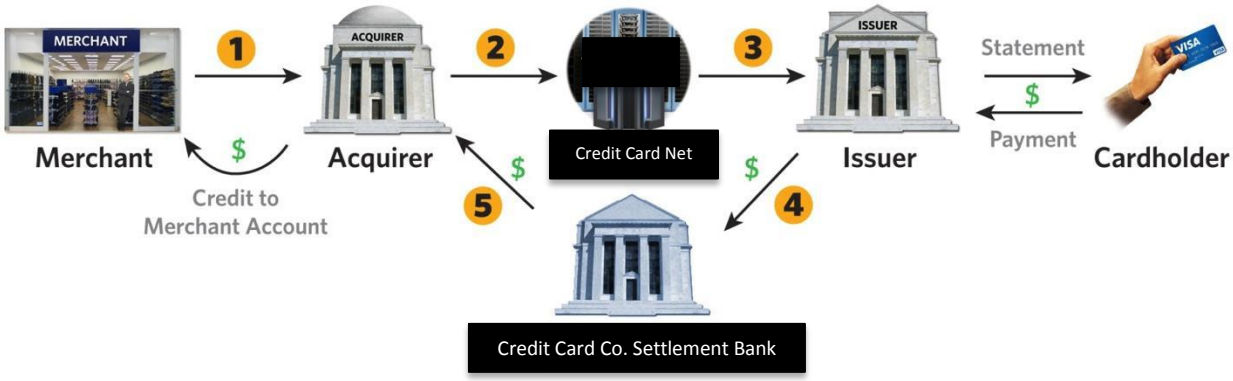
18. The Security Breach occurred as a result of Target's failure to implement reasonable and industry-standard security measures.

19. There are several parties to a typical credit or debit card transaction. The transaction begins when a cardholder uses a debit card or credit card at the point-of-sale system of a merchant (in this case Target). The point-of-sale system then transmits the card information (data encoded on the magnetic strip) to an acquiring bank(s), which the merchant contracts with to process the merchant's debit card and credit card transactions.

20. The acquiring bank(s) then transmits the card information and a request message to a processor; generally, the card company, such as Visa, MasterCard, or American Express. The processor then routes the request to an issuing bank for review and approval.

21. The issuing bank is the financial institution that issued the credit or debit card directly to the consumer. Plaintiffs and the other Class members are issuing banks. If the transaction is approved, the issuing bank will post the transaction to the consumer's credit card or debit card account.

22. The chart below graphically depicts an example of such a credit transaction:



23. Credit card companies require merchants, such as Target, to comply with certain regulations aimed at safeguarding customer information (generally, "Credit Card Operating Rules"). Credit Card Operating Rules generally prohibit the retention and storage of cardholder information subsequent to the authorization of the transaction.

24. For example, Visa's International Operating Regulations Core Principles for October 2013, provides:

> [t]o protect all parties to the Visa system, participants with access to personal Visa account information or Visa transaction information are responsible for following rigorous standards for data protection set by Visa. These standards may be consistent with or exceed industry standards. For example, the storage of magnetic-stripe data is strictly prohibited. … Participants in the Visa system agree to take

> appropriate measures to prevent the Visa system from being used for or associated with illegal activities.

25. On information and belief, Target was not in compliance with one or more Credit Card Operating Rules relating to the secure processing and storage of credit card and debit card information at the time of the Security Breach.

26. In 2006, Visa, MasterCard, and other members of the payment card industry ("PCI") established the Security Standards Council ("PCI SSC"). The PCI SSC establishes Payment Card Industry Data Security Standards (PCI DSS) and Payment Application Data Security Standards ("PA-DSS"), which are a set of requirements designed to ensure that all companies, including merchants such as Target, that process, store, or transmit credit card and debit card information maintain a secure environment.

27. Target was obligated—as a condition of being permitted to process transactions through PCI companies—to fully comply with the PCI DSS and other PCI requirements concerning the security of customer credit card and debit card information.

28. On information and belief, Target's payment processing systems were not in compliance with PCI DSS and other PCI requirements at the time of the Security Breach.

29. As one PCI forensic investigator noted:

> For a hacker to be able to infiltrate Target's network and access the POS application, several PCI-DSS and PA-DSS controls must not have been implemented effectively. Thus, Target was not compliant during the time of the breach . . . .
>
> How can I be so sure? 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.[1]

[1] *See* Ericka Chickowski, *Target Breach Should Spur POS Security, PCI 3.0 Awareness*, DARK READING (Dec. 24, 2013) (quoting Ken Stasiak, CEO of SecureState) (available at: http://www.darkreading.com/risk/target-breach-should-spur-pos-security-p/240164960) (last accessed Jan. 27, 2014).

30. Target has recognized that debit card and credit card information is highly sensitive and must be protected. According to Target's December 11, 2013 Privacy Policy, "[b]y interacting with Target, [customers] consent to use of information that is collected or submitted as described in this privacy policy." Target states:

> We maintain administrative, technical and physical safeguards to protect your 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.

31. Target knew, or reasonably should have known, that its network payment processing systems were vulnerable to attack, absent implementation of reasonable and industry-standard security measures.[2]

32. As a result of the Security Breach, the credit card and debit card information of approximately 40 million individuals was compromised, placing such individuals at a substantially increased risk of credit card fraud, debit card fraud, and identity theft.

33. The credit card and debit card "track" data stolen in the Security Breach could be used by criminals to create copies of the compromised credit cards and debit cards and to make unauthorized charges to such cards.

34. Certain Target customers' credit card, debit card, and personal information have been made available for sale on black market websites as a direct result of the Security Breach.

[2] *See* Dr. Neal Krawetz, *Point-of-Sale Vulnerabilities* (Aug. 27, 2007), available at http://www.hackerfactor.com/papers/cc-pos-20.pdf (last accessed Jan. 27, 2014) (describing a hypothetical hacker attack on Target's POS Systems and highlighting Target's "highly vulnerable" POS Systems, including Target's policy of storing customer information beyond the time permitted for compliance with the PCI SSC protocols). Upon information and belief, Target was aware of the POS Systems' vulnerabilities described in Dr. Krawetz's publication in 2007. Dr. Krawetz's paper was accessed 17 times by a domain identified as belonging to Target and an employee of Target emailed Dr. Krawetz seeking permission to distribute the paper internally at Target, a request which Dr. Krawetz granted.

35. Additionally, certain Target customers' credit card and debit card information stolen in the Security Breach has already been used to make unauthorized purchases.

36. The Security Breach is not the first time Target's payment processing systems have been compromised. In 2005, Target was hacked by Albert Gonzalez and others—including two Russian accomplices—who launched a three-year digital rampage through the networks of Target, TJ Maxx, and about half a dozen other companies, absconding with data for more than 120 million credit and debit card accounts.[3]

37. A Target spokeswoman told Reuters that an "extremely limited" number of payment card numbers were stolen from Target by Gonzalez and his gang. The other companies were not as fortunate: TJX, Hannaford Brothers grocery chain, the Dave & Busters restaurant chain, Office Max, 7-Eleven, BJ's Wholesale Club, Barnes & Noble, JC Penney, and, most severely, Heartland Payment Systems, were hit hard.[4] TJX alone ended up settling with VISA issuing banks for $40.9 million.[5] Target Chairman and CEO, Greg Steinhafel, admitted that Target is aware of the damages caused by previous security breaches: "Well, the liability is going to play out over time. We know that from prior breaches."

III. Financial Institutions Have Been Harmed by Target's Failure to Implement Reasonable and Industry-Standard Security Measures

38. Financial institutions, including Plaintiffs and other Class Members, have suffered losses resulting from the Security Breach relating to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest in

[3] Kim Zetter, *Target Got Hacked in 2005. Here's Why They Let It Happen Again*, WIRED (Jan. 17, 2014), available at: http://www.wired.com/threatlevel/2014/01/target-hack/?cid=co17243244&mbid=social17193574 (last accessed Jan. 27, 2014).
[4] *Id.*
[5] Ross Kerber, *Target Data Breach Could be Costly for Payment Partners*, REUTERS (Jan. 14, 2014), available at: http://www.reuters.com/article/2014/01/15/us-target-databreach-banks-idUSBREA0E03F20140115 (last accessed Jan. 27, 2014).

transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer confusion; and f) lost customers.

39. As a result of the Security Breach, in order to protect its customers and avoid fraud losses, CommunityBank reissued and mailed replacement cards to affected customers and placed a temporary purchase limit restriction of $1,000 per day on affected customers' cards until they received and activated their new card.

40. CommunityBank has also incurred losses as a result of the Security Breach on account of reimbursing customers for fraudulent charges, as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; lost interest in transaction fees, including lost interchange fees; incurring administrative expenses and overhead charges associated with monitoring and preventing fraud and responding to customer confusion; and lost customers.

41. FNBT incurred losses resulting from the Security Breach on account of reissuing and mailing new payment cards to customers; reimbursing customers for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; lost interest in transaction fees, including lost interchange fees; incurring administrative expenses and overhead charges associated with monitoring and preventing fraud and responding to customer confusion; and lost customers.

42. Numerous other Class members issued and sent replacement cards as a result of the Security Breach. JPMorgan Chase alone is reported to have replaced nearly 2,000,000 cards as a result of the Security Breach.

43. Replacing a credit card or debit card can cost a financial institution as much as $10 to $12 per card and sometimes in excess of these amounts.

44. A survey report from the Credit Union National Association (CUNA) is showing that the costs of the Security Breach are spreading to credit unions. The survey shows that credit unions have already had to absorb $25 million to $30 million in costs due to the Security Breach.[6]

45. Additionally, scams have reportedly been attempted to take advantage of the security concerns arising from the Security Breach. For instance, scammers have sent e-mails designed to appear to be from Target to Target customers in an attempt to trick the customers into divulging sensitive financial information. The scope of these so-called "phishing" campaigns is such that Target was forced to create a dedicated website containing transcripts of all official communications Target has sent customers following the Security Breach.

46. Beginning at least on December 19, 2013, Target knowingly burdened financial institutions when it began advising irate customers to call their banks instead of the Target customer services lines, because Target was not prepared to handle the complaints.

47. Target's Chairman and CEO publicly advised consumers to request a new card if they had concerns that credit monitoring was not enough. He also promised to send affected customers new cards and to even expedite them, if requested. He did not make it clear that Target could not send cards on behalf of issuing banks.[7]

[6] Jon C. Ogg, *Cost of Target Data Theft Spreads, Credit Unions Now . . . Banks Next?*, YAHOO FINANCE (Jan. 22, 2014), available at: http://finance.yahoo.com/news/cost-target-data-theft-spreads-193317887.html (last accessed Jan. 27, 2014).

[7] CNBC, *CNBC Transcript, Target Chairman and CEO Gregg Steinhafel Speaks with Becky Quick Today on CNBC* (Jan. 13, 2014), available at: http://www.cnbc.com/id/101331335#_gus (last accessed Jan. 27, 2014).

IV. Target Concedes It is Liable for Losses Suffered by Financial Institutions as a Result of the Security Breach

48. Target's Chairman and CEO publicly accepted responsibility for Target's failure in an interview with CNBC on January 13, 2014, stating: "Clearly, we're accountable and we're responsible."[8]

49. Target's Chairman and CEO also publicly promised that Target would be the only entity liable for fraudulent charges caused by the breach:

> BECKY (INTERVIEWER): When you say that there's zero liability, what does that mean? Is Target paying for that? Are the credit card companies paying for that? The banks?
>
> GREGG STEINHAFEL: Yeah, zero liability is zero liability, which means Target is paying for any—any possible fraudulent activity on anybody's credit card. And we're providing the—free credit monitoring service. So the guest has no liability whatsoever."[9]

50. Target's Chairman and CEO publicly acknowledged that Target is responsible for damages that financial institutions, including issuing banks, incurred as a result of the Security Breach:

> BECKY: What have the banks and credit card companies said? I mean, normally my credit card company would be the one who's responsible for picking up—fraudulent charges that would show up…What's JP Morgan had to say about this? What's Wells Fargo had to say? What's—what do Visa and Mastercard have to say about it?
>
> STEINHAFEL: Well, again, we're in the middle of this investigation. And we haven't—got to the end of the time—table. 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. And there'll be a package and aggregated and brought to us.[10]

[8] *See id.*
[9] *See id.*
[10] *See id.*

51. Target's Chairman and CEO also publicly stated that issuing banks were not wrong in the decision to issue new payment cards to consumers, whether proactively or upon request:

> Most of the industry came down on choice like we did. And J.P. Morgan and a few other took a different approach. I don't think any approach was wrong. I think everybody is just really well intentioned to try and do the right thing.[11]

52. Target's Chairman and CEO further stated that banks that proactively issued new cards to consumers were not incorrect, despite the backlash from inconvenienced consumers who were caught in the middle of holiday shopping:

> No, I mean, we're accountable. I mean, clearly we're accountable and we're responsible for that. So it's not up to us to—you know, to decide what policies are correct for any financial institution. We want to do the right thing. I mean, that—that's been the history of Target. It's been the 51 year of this—company. It's been do the right thing and support the business and support—partners the way that they want the business to support it. And that—that's our approach.[12]

53. Target's failure to safeguard customer personal and financial information was patently unreasonable, and has caused damage to Plaintiffs and the other Class members.

V. Target Failed to Promptly Notify Financial Institutions of the Security Breach

54. Upon information and belief, Target knew of the Security Breach as early as December 11, 2013.

55. On the morning of Sunday, December 15, 2013, Target's Chairman and CEO personally learned of the Security Breach.[13] By 6 o'clock p.m. on that same day, Target had eliminated the "malware and access points."[14]

56. On December 18, 2013, Brian Krebs, a security blogger at *KrebsOnSecurity* ("Krebs"), announced that Target was investigating a data breach involving an unknown number of Target

[11] *See id.*
[12] *See id.*
[13] *See id.*
[14] *See id.*

customers who shopped at the company's brick-and-mortar stores from November 27, 2013 through December 15, 2013.[15]

57. On December 19, 2013, Target finally confirmed that it was aware of unauthorized access to payment card data that impacted customers making credit card and debit card purchases in its United States' stores. Target estimated that approximately 40 million credit card and debit card accounts had been affected.

58. The December 19, 2013 notification only identified potentially impacted customers as those who shopped in its U.S. stores between November 27, 2013 and December 15, 2013.

59. On December 20, 2013, Target announced that the Security Breach occurred between November 27, 2013 and December 15, 2013. At that time, Target assured the public that there was "no indication that PIN numbers have been compromised" and that customers would not be liable for fraudulent charges—those would be the responsibility of Target or the customers' banks.[16]

60. On December 27, 2013, Target issued an announcement that encrypted PIN data had been removed from its system, a fact it previously denied.

61. On January 10, 2014, in an additional and separate announcement, Target announced that the personal information—names, mailing addresses, telephone numbers, and email addresses—of 70 million individuals was stolen as a result of the Security Breach. This stolen information is in addition to the credit card and debit card information of 40 million individuals that Target previously disclosed.

---

[15] Brian Krebs, *Sources: Target Investigating Data Breach* (Dec. 18, 2013), KREBS ON SECURITY, available at: http://www.krebsonsecurity.com/2013/12/sources-Target-investigating-data-breach (last accessed Jan. 27, 2014).

[16] Target, *A Message from CEO Gregg Steinhafel About Target's Payment Card Issues* (Dec. 20, 2013), available at: https://corporate.Target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca (last accessed Jan. 27, 2014).

62. The same day, Target offered one year of free credit monitoring to customers who shopped at its U.S. stores.

CLASS ACTION ALLEGATIONS

63. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), Plaintiffs bring this action on behalf of a class defined as follows:

> All banks, credit unions, and other financial institutions in the United States, including its territories and protectorates, that have suffered injury as a result of Target's failure to secure the personal and financial information of its customers from approximately November 27, 2013 through December 15, 2013.

64. Plaintiffs are members of the Class they seek to represent.

65. This action is brought and may properly be maintained as a class-action pursuant to 28 U.S.C. § 1332(d). This action satisfies the procedural requirements set forth in Fed. R. Civ. P. 23.

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

a. Whether Target failed to employ reasonable and industry-standard measures to secure and safeguard its customers' credit card, debit card and personal information;

b. Whether Target unlawfully retained credit card and debit card information in violation of Minn. Stat. Ann. §325E.64;

c. Whether Target properly implemented and maintained its purported security measures to protect its customers' credit card, debit card and personal information;

d. Whether Target misrepresented that it did not retain customer financial information and misrepresented that its customers' financial and personal information was secure;

e. Whether Target's security failures resulted in Target's customers' financial and personal information being accessed and disseminated by thieves;

f. Whether Target was negligent in failing to properly secure and protect its customers' financial and personal information;

g. Whether Plaintiffs and other members of the Class are entitled to injunctive relief; and

h. Whether Plaintiffs and other members of the Class are entitled to damages and the measure of such damages.

67. Plaintiffs' claims are typical of the claims of the Class Members. Plaintiffs and all Class Members were damaged by the same unreasonable conduct of Target.

68. Plaintiffs will fairly and adequately protect and represent the interests of the Class. The interests of Plaintiffs are coincident with, and not antagonistic to, those of the Class.

69. Plaintiffs have retained counsel competent and experienced in complex class action litigation.

70. Members of the Class are so numerous that joinder is impracticable. Plaintiffs believe that there are hundreds, if not thousands, of Class members.

71. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual Class members, because Target has acted on grounds generally applicable to the entire Class. Thus, determining damages with respect to the Class as a whole is appropriate.

72. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated entities to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender.

73. Plaintiffs know of no special difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

COUNT ONE
Violation of Minnesota Statute Annotated § 325E.64

74. Plaintiffs incorporate by reference each of the preceding paragraphs as if fully set forth herein.

75. Defendant is a Minnesota corporation subject to Minn. Stat. Ann. §325E.64 Subd. 2, which provides as follows:

> 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.

76. Minn. Stat. Ann. §325E.64 Subd. 3 provides that a violator of this section that experiences a security breach must reimburse reasonable costs incurred by financial institutions as a result of the breach.

> 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, including but not limited to, any cost incurred in connection with:
>
> (1) the cancellation or reissuance of any access device affected by the breach;
>
> (2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;
>
> (3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;
>
> (4) any refund or credit made to a cardholder to cover the cost of any

> unauthorized transaction relating to the breach; and
>
> (5) the notification of cardholders affected by the breach.
>
> The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

77. Target improperly and in contradiction and violation of Minn. Stat. Ann. §325E.64 retained its customers' credit card and debit card information, including security code data, PIN verification codes, and the full content of "track" credit card and debit card data, subsequent to authorization of its customers' transactions using such cards and, in the case of PIN debit card transactions, retained such information subsequent to 48 hours after authorization of such transactions.

78. Plaintiffs and the other Class Members have incurred substantial costs as a result of the Security Breach in order to protect the information of their cardholders and to continue to provide services to their cardholders.

79. Pursuant to Minn. Stat. Ann. §325E.64 Subd. 3, Target is obligated to reimburse Plaintiffs and the other Class members for their reasonable costs and damages.

COUNT TWO
Negligence

80. Plaintiffs incorporate by reference each of the preceding paragraphs as if fully set forth herein.

81. Target had an affirmative duty to exercise reasonable care in safeguarding and protecting its customers' financial and personal information, including credit card and debit card information.

82. Target breached its duty to exercise reasonable care in failing to implement reasonable and industry-standard security measures to protect its customers' credit card, debit card, and personal information.

83. It was foreseeable that Target's failure to exercise reasonable care in protecting its customers' credit card, debit card, and personal information would result in Plaintiffs and the other Class members suffering losses related to: a) the expense of creating, issuing, and mailing new payment cards to their customers.; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest in transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer confusion; and f) lost customers.

84. As a direct result of Target's failure to secure and protect its customers' credit card, debit card, and personal information, Plaintiffs and the other Class members were damaged on account of suffering losses related to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest in transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer confusion; and f) lost customers.

85. Target's wrongful actions and/or inaction (as described above) constituted negligence at common law.

COUNT THREE
Negligent Misrepresentation

86. Plaintiffs incorporate by reference each of the preceding paragraphs as if fully set forth herein.

87. Millions of Target's customers made purchases at Target stores with credit cards and debit cards issued by Plaintiffs and the other Class Members. Target represented to Plaintiffs and Plaintiffs' customers that it would safeguard and protect its customers' financial and personal information from harm. Credit Card Operating Rules and PCI standards provide reasonable commercial standards for safeguarding and protecting customer credit card and debit card information from harm.

88. Target's promises to safeguard and protect its customers' financial and personal information were material facts upon which Plaintiffs and other Class members relied.

89. Target was not in compliance with one or more Credit Card Operating Rules and PCI Standards at the time of the Security Breach, and was not properly safeguarding customer data.

90. Plaintiffs and the other Class members reasonably relied on Target to comply with the Credit Card Operating Rules and PCI standards, and Target's representations that it would safeguard customer data.

91. Plaintiffs and the other Class members suffered actual damages as a result of Target's negligent misrepresentations.

COUNT FOUR
Negligent Performance of Services

92. Plaintiffs incorporate by reference each of the preceding paragraphs as if fully set forth herein.

93. Target had a pecuniary interest in processing its customers' credit card and debit card transactions.

94. In addition to its pecuniary interests, Target processed its customers' credit card and debit card transactions for the benefit of assigning banks, credit card companies, and issuing banks—including Plaintiffs and the other Class members—which also had a pecuniary interest in such transactions.

95. Plaintiffs and the other Class members relied upon Target exercising reasonable care in processing credit card and debit card transactions and in ensuring that sensitive credit card and debit card information remained secure.

96. Target failed to exercise reasonable care in processing credit card and debit card transactions on account of its failure to implement reasonable and industry-standard security measures.

97. Plaintiffs and the other Class members suffered actual damages as a result of Target's failure to exercise reasonable care in processing credit card and debit card transactions.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request that the Court:

A. Determine that this action may be maintained as a class action pursuant to Federal Rule of Civil Procedure 23(a), (b)(2) and (b)(3);

B. Direct that reasonable notice of this action, as provided by Federal Rule of Civil Procedure 23(c)(2), be given to the Class;

C. Appoint Plaintiffs as Class Representatives;

D. Appoint Plaintiffs' counsel as Class Counsel;

E. Enter judgment against Target and in favor of Plaintiffs and the Class;

F. Adjudge and decree under Fed. R. Civ. P. 57 and 18 U.S.C. § 2201(a) that the acts alleged herein by Target were in violation of Minn. Stat. Ann. § 325E.64 and constitute negligence, negligent misrepresentations, and negligent performance of services;

G. Award all compensatory and statutory damages to Plaintiffs and the Class in an amount to be determined at trial;

H. Award punitive damages, including treble and/or exemplary damages, in an appropriate amount;

I. Enter an injunction permanently barring continuation of the conduct complained of herein, and mandating that Target be required to adopt and implement appropriate systems, controls, policies and procedures to ensure Target remains in compliance with duties required by law and industry standards, and further mandating that the Target install such systems, controls, policies and procedures implemented to achieve full remuneration and relief to the Plaintiffs and the Class;

J. Award Plaintiffs and the Class the costs incurred in this action together with reasonable attorneys' fees and expenses, including any necessary expert fees as well as pre-judgment and post-judgment interest; and

K. Grant such other and further relief as is necessary to correct for the effects of Target's unlawful conduct and as the Court deems just and proper.

JURY TRIAL DEMAND

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

DATED: January 29, 2014

Respectfully submitted,

s/ Rhett A. McSweeney

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

Ben Barnow
Erich P. Schork
BARNOW AND ASSOCIATES, P.C.
1 North LaSalle Street, Suite 4600
Chicago, IL 60602
(312) 621-2000 (p)
(312) 641-5504 (f)
b.barnow@barnowlaw.com
e.schork@barnowlaw.com

Don Barrett
BARRETT LAW GROUP, P.A.
404 Court Square North
Lexington, Mississippi 39095-0927
(662) 834-9168 (p)
(662) 834-2628 (f)
dbarrett@barrettlawgroup.com

Dewitt M. Lovelace
LOVELACE & ASSOCIATES, P.A.
12870 U.S. Hwy. 98, W. Suite 200
Miramar Beach, FL 32550
(850) 837-6020 (p)
(850) 837-4093 (f)
dml@lovelacelaw.com

Mike Roberts
ROBERTS LAW FIRM, P.A.
20 Rahling Circle
P.O. Box 241790
Little Rock, AR 72223-1790
(501) 821-5575 (p)
(501) 821-4474 (f)
mikeroberts@robertslawfirm.us

Thomas Walter Umphrey
Michael A. Havard
PROVOST UMPHREY LAW FIRM, LLP
490 Park Street, PO Box 4905
Beaumont, Texas 77701
(409) 299-5178 (p)
(409) 838-8888 (f)

COUNSEL FOR PLAINTIFFS