UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

PUTNAM BANK, Individually and on behalf of a class of all similarly situated financial institutions, Plaintiffs, v. TARGET CORPORATION, Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Putnam Bank individually and on behalf of a class of all similarly situated financial institutions, asserts the following in this Class Action Complaint against Target Corporation ("Target" or "Defendant").

NATURE OF THE ACTION

1. On or about November 23, 2013, in one of the largest data security breaches ever to have occurred in the United States, approximately ***110 million*** credit cards and debit cards were compromised because of Target's acts and omissions. Plaintiff brings this class action on its own behalf and on behalf of all other similarly situated financial institutions seeking damages resulting from Target's misrepresentations, unfair and deceptive acts and practices, negligence, breach of contract, and improper retention of certain customer confidential information with respect to the data security breach. Target's failure to adequately safeguard customer confidential information and related data and Target's failure to maintain adequate

encryption, intrusion detection, and prevention procedures in its computer systems caused the losses hereinafter set forth.

2. Target delayed notifying consumers of the security breach until almost ***four weeks after the breach occurred***, and only after a respected security blogger publicly reported the breach on December 18, 2013. In fact, Target only initially estimated that the data breach would impact 40 million of its customers.

3. A day later, Target began disclosing to the public that an unauthorized access to Target payment card data had occurred that "may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013" and "customer name, credit or debit card number, and the card's expiration date and CVV" may have been involved.[1]

4. According to a Target spokeswoman, "[a]t this stage, the company's approach to outreach has been using social media, email news coverage to alert customers, rather than targeting particular customers who may have been affected."[2]

5. As of December 20, 2013, sources report that the credit and debit card accounts that were used by Target customers during the relevant time period and were stolen by thieves "have been flooding underground back markets in recent weeks, selling

[1] *See* https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca. (All website citations were last visited on January 13, 2014.).

[2] http://articles.economictimes.indiatimes.com/2013-12-20/news/45419033_1_molly-snyder-target-spokeswoman-credit-reports.

in batches of one million cards and going for anywhere from $20 to more than $100 per card."[3]

6. Then, on January 10, 2014, Target announced that the number of customers affected by its data breach was approximately ***110 million***, almost ***triple*** its previous estimate.[4] Worse, Target also belatedly announced that "[i]n addition to the already-known customer names, card numbers, expiration dates and the CVV three-digit security codes that were stolen . . . the new information included in the breach now includes names, mailing address, phone numbers and email address . . . ."[5]

7. In fact, Target acknowledged that the 110 million figure could include information from customers who did not even swipe their debit or credit cards during the period. The data "involves all kinds of customer information that Target had collected over time. Those customers need not have even shopped at Target during the holiday season to have had their information stolen."[6]

8. As a result of Target's wrongful conduct, sensitive customer information was accessed from Target's computer systems. As a direct and proximate result of the data breach, and after being notified of the data breach, Plaintiff and members of the

[3] *See* http://krebsonsecurity.com/tag/target-data-breach/.

[4] http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?hpw&rref=business&_r=0.

[5] http://www.foxbusiness.com/industries/2014/01/10/target-guest-info-also-stolen-in-black-friday-breach/.

[6] http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?hpw&rref=business&_r=0.

proposed Class have been damaged as they have had notify its customers of the data compromise and to reissue new credit and debit cards to their customers.

9. Given the magnitude of the data breach, Target's wrongful conduct caused Class member financial institutions to incur significant losses associated with credit and debit reissuance; customer reimbursement for fraud losses; lost interest and transaction fees (including lost interchange fees); lost customers; administrative expenses associated with monitoring and preventing fraud and administrative expenses in dealing with customer confusion; fraud claims; and card reissuance.

10. Plaintiff seeks to recover damages caused by Defendant's negligent misrepresentations, unfair and/or deceptive acts or practices in violation of Minn. Stat. Ann. §325F.69 Subd. 1, violation of Minn. Stat. Ann. §325E.64, negligence, and breach of contract.

11. Plaintiff also seeks a finding that Defendant improperly retained customer data and injunctive relief enjoining Defendant from such improper retention.

JURISDICTION AND VENUE

12. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d), in that: (a) the Class (as defined below) has more than 100 Class members; (b) the amount at issue exceeds five million dollars ($5,000,000.00), exclusive of interest and costs; and (c) minimal diversity exists as Plaintiff and Defendant are citizens of different states.

13. Defendant is subject to the provisions of Minn. Stat. Ann. §325F.69 Subd. 1 in that the unfair or deceptive acts or practices complained of occurred primarily and

substantially within the State of Minnesota. Defendant is further subject to the provisions of Minn. Stat. Ann. §325E.64 in that the data breach complained of herein occurred primarily and substantially within the State of Minnesota.

14. Venue in the United States District Court for the District of Minnesota is appropriate, pursuant to 28 U.S.C. §1391(a), in that Defendant resides and is headquartered and incorporated in the District of Minnesota, and a substantial part of the events or omissions giving rise to the claim occurred in the District of Minnesota.

PARTIES

15. Plaintiff Putnam Bank is a federally-charted community bank headquartered in Putnam, Connecticut.

16. Defendant Target Corporation is a Minnesota corporation with its principal place of business located in Minneapolis, Minnesota. Target does business throughout the State of Minnesota and the United States.

CLASS ACTION ALLEGATIONS

17. Plaintiff brings this action on its own and on behalf of all other financial institutions similarly situated for the purpose of asserting claims alleged herein on a common basis, pursuant to 28 U.S.C. §1332(d). The proposed Class (the "Class") is defined as:

> Financial institutions that have suffered damages and/or harm as a result of data breaches set forth herein with respect to personal and financial information of customers who used debit or credit cards at Target's retail stores.

18. Plaintiff Putnam Bank is a member of the Class it seeks to represent.

19. 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.

20. The conduct of Defendant has caused injury to members of the proposed Class. The proposed Class is so numerous that joinder of all members is impracticable.

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

a. Whether Defendant failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;

b. Whether Defendant negligently misrepresented that it did not retain customer financial information and negligently represented that it provided security as to its computer systems to prevent intrusions;

c. Whether the conduct (action or inaction) of Defendant resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;

d. Whether Defendant knew or should have known of the vulnerability of its computer systems to breach;

e. Whether Defendant knew or should have known of the risks to financial institutions inherent in failing to protect such financial and personal information;

f. Whether Defendant improperly retained customer personal and financial information despite representations that it would not keep such information;

g. Whether Defendant disclosed (or directly or indirectly caused to be disclosed) private financial and personal information of customers;

h. Whether Defendant engaged in unfair and deceptive acts or practices as set forth in Minn. Stat. Ann. §325F.69 Subd. 1;

i. Whether Defendant violated Minn. Stat. Ann. §325E.64;

j. Whether Plaintiff and members of the proposed Class have been injured by Defendant's negligent misrepresentations, violations of Minnesota law, negligence, and/or breach of contract;

k. Whether Plaintiffs and members of the proposed Class have been damaged by the conduct of Defendant;

l. Whether Defendant's violations of Minnesota law were knowing, willful, wanton, intentional, deliberate, and/or malicious or otherwise caused proximate damages to Plaintiff and the Class such that Plaintiff and Class members are entitled to an award of multiple or punitive damages and attorneys' fees;

m. Whether Defendant breached its duties to exercise reasonable and due care in obtaining, using, retaining, and safeguarding the personal and financial information of bank customers; and

n. Whether Defendant breached its obligations to Plaintiff and Class members as third party beneficiaries under Defendant's contract with an acquiring bank.

22. Plaintiff's claims are typical of the proposed Class. The same events and conduct that give rise to Plaintiffs' claims and legal theories also give rise to the claims and legal theories of the proposed Class.

23. Plaintiff will fairly and adequately represent the interests of the proposed Class. There are no disabling conflicts of interest between Plaintiff and the proposed Class.

24. Plaintiff is part of the putative Class, possesses the same interests, and suffered the same injuries as Class members, making its interests coextensive with those of the Class. The interests of Plaintiff and the proposed Class are aligned so that the motive and inducement to protect and preserve these interests are the same for each.

25. Common questions of law and fact predominate over individualized questions. A class action is superior to other methods for the fair and efficient adjudication of this controversy.

26. Plaintiff is represented by experienced counsel who are qualified to handle this case. The lawsuit will be capably and vigorously pursued by Plaintiff and its counsel.

FACTUAL BACKGROUND

The Data Breach and Subsequent Sale of Credit and Debit Card Information

27. Target is the second largest discount retailer in the United States and has more than 1,795 stores nationwide.

28. On December 18, 2013, Brian Krebs, of Krebs On Security ("Krebs"), publicly announced that Target was investigating a data breach potentially involving millions of customer credit and debit card records. The information – based upon multiple reliable sources – included two different top 10 credit card issuers reporting that the data breach, extending to nearly all Target locations nationwide, involved the theft of data stored on the magnetic strip of cards used at the stores. Target did not respond to multiple requests for comment.[7]

29. The following day, Target began to provide limited information to the public regarding the data breach, although it did not notify those who may actually be affected.

30. Experts reported the theft as the "second-largest credit card breach in U.S. history[.]"[8]

31. The theft of approximately 40 million Target customers' information (later updated to 110 million Target customers, see ¶48, *infra*) has significantly exposed those customers to the threat of substantial harm. Sources confirm that the thieves have taken

[7] http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach.

[8] http://www.boston.com/2013/12/20/fury-and-frustration-over-target-data-breach/LAEw7wmAeKBl0MJk0lBRDL/story.html.

the stolen data from the magnetic strips on the backs of Target customer credit and debit cards and attempted to sell the information on underground markets.

32. For example, on December 20, 2013, The New York Times reported that:

> On Dec. 11, one week after hackers breached Target's systems, Easy Solutions, a company that tracks fraud, noticed a ten- to twentyfold increase in the number of high-value stolen cards on black market web sites, from nearly every bank and credit union.
>
> The black market for credit card and debit card numbers is highly sophisticated, with numerous card-selling sites that are indistinguishable from a modern-day e-commerce site. Many sell cards in bulk to account for the possibility of cancellations. Some go for as little as a quarter. Corporate cards can sell for as much as $45.
>
> But the security blogger Brian Krebs, who first broke news of the Target security breach on his website, said some Target customers' high-value cards were selling for as much as $100 on exclusive black market sites.[9]

33. A fraud analyst at a major bank said his team had independently confirmed that Target had been breached after buying a huge chunk of the bank's card accounts from a well-known "card shop" – an online store advertised in cybercrime forums as a place where thieves can reliably buy stolen credit and debit cards.[10]

34. According to Krebs, there are literally "hundreds of these shady stores selling stolen credit and debit cards from virtually every bank and country. But this store has earned a special reputation for selling quality 'dumps,' data stolen from the magnetic stripe on the backs of credit and debit cards. Armed with that information, thieves can

[9] http://bits.blogs.nytimes.com/2013/12/20/target-customer-information-shows-up-on-the-black-market/?_r=0.

[10] http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/#more-24093.

effectively clone the cards and use them in stores. If the dumps are from debit cards and the thieves also have access to the PINs for those cards, they can use the cloned cards at ATMs to pull cash out of the victim's bank account." *Id.*

35. At least two sources and major banks said they had heard from the credit card companies:

> More than a million of their cards were thought to have been compromised in the Target breach. One of those institutions noticed that one card shop in particular had recently alerted its loyal customers about a huge new batch of more than a million quality dumps that had been added to the online store. Suspecting that the advertised cache of new dumps were actually stolen in the Target breach, fraud investigators with the bank browsed this card shop's wares and effectively bought back hundreds of the bank's own cards.
>
> When the bank examined the common point of purchase among all the dumps it had bought from the shady card shop, it found that all of them had been used in Target stores nationwide between Nov. 27 and Dec. 15. Subsequent buys of new cards added to that same shop returned the same result.[11]

36. The information provided by the card shops includes city, state, and zip code. According to a fraud expert, that feature "allows customers of the shop to buy cards issued to cardholders that live nearby. This lets crooks who want to use the cards for in-store fraud avoid any knee-jerk fraud defenses in which a financial institution might block transactions that occur outside the legitimate cardholder's immediate geographic region."[12]

[11] http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/.

[12] https://krebsonsecurity.com/2013/12/non-us-cards-used-at-target-fetch-premium.

37. On December 20, 2013, a card shop announced the availability of a new base – "Barbarossa" – which consists of more than 330,000 debit and credit cards issued by banks in Europe, Asia, Latin America, and Canada. Krebs reported that "[a]ccording to one large bank in the U.S. that purchased a sampling of cards across several countries – *all of the cards in the Barbarossa base also were used at Target during the breach timeframe*." *Id.* (emphasis in original). The cards for sale in the Barbarossa base vary widely in price from $23.62 per card to as high as $135 per card.[13]

38. Nicole Perloth of *The New York Times* wrote:

> Credit and debit card numbers often sell in bulk on black market websites. Platinum cards can fetch as much as $35 and corporate cards $45. That stolen data — someone's financial identity — can be burned onto magnetic strips on counterfeit cards that can be used for fraudulent purchases, or to buy gift cards that can be exchanged for cash.[14]

39. Beth Givens, who runs the San Diego-based Privacy Rights Clearinghouse, said the biggest threat is for people who shopped at Target using debit cards, where money comes directly out of their checking accounts. She said laws are less protective of people who use debit cards, and someone's PIN number could mean unauthorized access at an ATM. "If you used a debit card at Target, I would recommend that you cancel it,"

[13] "The prices seem to be influenced by a number of factors, including the issuing bank, the type of card (debit or credit), how soon the card expires, and whether the card bears a special notation that often indicates a higher credit limit, such as a Platinum card." https://krebsonsecurity.com/2013/12/non-us-cards-used-at-target-fetch-premium.

[14] http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html.

she said. "With a debit card you risk having your checking account wiped out. It will certainly be replenished, but it may take several weeks."[15]

40. The thieves could use magnetic stripe data to create counterfeit payment cards. The *Wall Street Journal* notes that crime rings often use these counterfeits to purchase gift cards at major retailers and then convert them back to cash. The attackers could also withdraw cash from ATMs if they managed to steal PIN data from debit transactions, Krebs on Security notes.[16]

41. According to a senior payments executive, the hackers who attacked Target also managed to steal the encrypted personal identification numbers (PINs) of debit card users.[17] One major U.S. bank fears that the thieves would be able to crack the encryption code and make fraudulent withdrawals. *Id.*

42. When Target finally announced the data breach on December 18, 2013, it originally pointed consumers to the three credit reporting agencies – Equifax, Trans Union, and Experian – to place fraud alerts on their accounts. Givens said that would give a false sense of security, because it would not solve the problem of someone being able to use the customer's credit or debit card. Those alerts, she said, are best for when someone's Social Security number is compromised. With that piece of data, a savvy enough thief could get a loan for a car or a house. Givens further explained:

---

[15] http://www.utsandiego.com/news/2013/dec/19/target-data-breach-consumers-credit-debit-fraud/all/?print.

[16] http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/#ixzz2o8crqsYH.

[17] http://finance.yahoo.com/news/exclusive-target-hackers-stole-encrypted-054416116.html?soc.

> "Establishing a fraud alert, establishing a security freeze and ordering your free credit report are not appropriate tips for this type of fraud," she said. "The only way it ends up on the credit report is if somebody goes on a shopping spree of a lifetime and then you for some reason don't read account statements and it lingers for months, and then Target or the credit card company reports it to credit bureaus."
>
> While getting someone's credit card number can't automatically lead to a Social Security number, Larson said it could lead to a scheme called phishing. That's where a thief would contact a person, pretending to be from a bank or credit card company, establishing credentials using the personal information they have stolen. Then they would try to trick that person into giving up the Social Security number or other information that can be used to establish new accounts.
>
> "Then they'd have a complete puzzle of who you are," he said. "It's very important to know that a consumer may be victim of further attack."[18]

43. On December 20, Target announced on its website that it would offer free credit monitoring services for everyone impacted but did not advise how consumers could take advantage of the offer: "We'll be in touch with you soon on how and where to access the service."[19]

44. According to the Privacy Rights Clearinghouse, credit monitoring services cannot protect against, *e.g.*, existing account fraud *(i.e.*, when an imposter uses your current accounts to commit fraud); debit or check card fraud (*i.e.*, when an imposter uses your debit card or check card (or a "cloned" card or the information from your card) to

[18] http://www.utsandiego.com/news/2013/dec/19/target-data-breach-consumers-credit-debit-fraud/all/?print.

[19] https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca/?v=1B1FB121913#sf20816856.

remove money from your bank account; criminal identity theft (*i.e.*, when an imposter gives another person's name and personal information (or counterfeit documents) to a law enforcement officer during an arrest; and medical identity theft (*i.e.*, when an imposter uses an individual's name and/or other information, often insurance information, to obtain or make false claims for medical goods or services).[20]

45. Several attorneys general have questioned Target's security system and its delay in responding to the massive data breach.

46. On December 19, 2013, Connecticut Attorney General George Jepsen pressed Target for more information. The incident, he said, "raises questions about the effectiveness of Target's measures to protect the confidentiality and security of private information it receives from its customers."[21]

47. United States Senator Richard Blumenthal said in a statement that he was concerned that Target did not act as quickly as it should have to protect customers. "Notification should be immediate and comprehensive," he said. *Id.*

48. Then, on January 10, 2014, Target announced that the number of impacted customers was approximately ***110 million***, nearly ***triple*** what the Company initially estimated. Target also announced that in the data breach, customer names, mailing addresses, phone numbers, and email addresses were compromised.

[20] https://www.privacyrights.org/identity-theft-monitoring-services.

[21] http://www.courant.com/business/hc-target-credit-card-data-breach-20131219,0,7507959.story.

49. Furthermore, some of the impacted individuals may not have even swiped their debit or credit cards at Target stores during the holiday season. Rather, Target disclosed that the breach included customer data collected over time, thereby indicating that Target had been wrongfully storing customer information.

How a Credit or Debit Card Transaction Works and the Governing Standards

50. A typical credit or debit card transaction made on a credit card network is processed through a merchant (where the initial purchase is made), an acquiring bank (which is typically a financial institution that contracts with a merchant to process its credit card and debit card transactions, and is a member of the credit card associations),[22] a processor, and an issuer (which is a financial institution – like the Plaintiff and members of the proposed Class – that issues credit cards and debit cards to consumers and is a member of the credit card associations). When a purchase is made using a credit card or debit card on a credit card network, the merchant seeks authorization from the issuer for the transaction. In response, the issuer informs the merchant whether it will approve or decline the transaction. Assuming the transaction is approved, the merchant processes the transaction and electronically forwards the receipt directly to the acquiring bank. The acquiring bank then pays the merchant, forwards the final transaction data to the issuer, and the issuer reimburses the acquiring bank. The issuer then posts the charge to the consumer's credit card or debit card account.

[22] Plaintiff believes that it will be able to identify the acquiring bank with whom Target contracted after an opportunity for discovery.

51. In accordance with their rules, regulations and operating procedures, credit card companies monitor their respective networks for potential fraudulent activity. When suspected fraudulent use of credit cards and/or debit cards is identified, credit card companies issue alerts to the issuing banks. Upon information and belief, these alerts generally set forth the type of compromised data, the relevant timeframe of the compromise and a list of card numbers that have been exposed.

52. Plaintiff and members of the proposed Class serve as issuing banks, which issue debit cards to their customers.

53. Target, a seller of retail goods, accepts credit and debit card transactions from consumers.

54. Upon information and belief, Target had a contract with an acquiring bank for the processing of credit card transactions on behalf of Target.

55. Target, the acquiring bank, and various credit card companies together participate in systems whereby consumers may purchase goods from Target retail stores using their credit cards.

56. The credit card companies issue regulations ("Card Operating Regulations") that governed the conduct of Target at all times relevant to this action.

57. Target's contract with the acquiring bank requires Target to comply with the Card Operating Regulations.

58. Target is required to comply with the Card Operating Regulations, including those portions of the Card Operating Regulations that mandate safeguarding of cardholder information and that prohibit retention or storage of credit cardholder account

numbers, personal information, magnetic strip information, or credit card transaction information subsequent to the card authorization.

59. Target must also comply with the Payment Card Industry Data Security Standard (the "PCI Standards"). The PCI Standards require the following:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored data
- Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security

60. At all times relevant hereto, Target knew or should have known that the Card Operating Regulations forbid it from retaining or storing credit card magnetic strip information subsequent to the authorization of a transaction.

61. At all times relevant hereto, Target knew or should have known that the Card Operating Regulations forbid it from disclosing any credit cardholder account numbers, personal information, magnetic strip information, or transaction information to third parties other than the merchant's agent, the acquiring bank, or the acquiring bank's agents.

62. At all times relevant hereto, Target knew or should have known that the Card Operating Regulations require it to secure and keep confidential credit cardholder information and magnetic strip information from unauthorized disclosure, as set out in the Card Operating Regulations.

63. Target's contract with the acquiring bank and its involvement in this complex web of interrelated financial intuitions required that Target: (a) comply with the Card Operating Regulations; (b) properly secure credit card magnetic strip information;

(c) not retain or store such information subsequent to authorization of a transaction; and (d) not disclose such information to unauthorized third parties.

Target Fails to Safeguard Customer Information in Contravention of Applicable Standards

64. Target, at all times relevant to this action, represented and had a duty to Plaintiff and members of the proposed Class to: (a) comply with the Card Operating Regulations; (b) properly secure credit card magnetic strip information; (c) not retain or store such information subsequent to authorization of a transaction; and (d) not disclose such information to unauthorized third parties.

65. As indicated by news reports, Target retained magnetic strip information/data from millions of credit and debit cards issued by Plaintiff and members of the proposed Class to their customers.

66. Target negligently allowed credit card magnetic strip information to be compromised.

67. Target negligently utilized a computer system that retained, stored, and/or disclosed (or allowed to be disclosed) credit card magnetic strip information.

68. Data from the magnetic strip on millions of credit cards, issued by banks to their customers and used by those customers at Target stores, was accessed or obtained by third parties from Target.

69. Third parties were able to access, obtain, and use the credit card magnetic strip information to fraudulently make transactions and to sell, transfer, use, or attempt to use such information for fraudulent purposes.

70. Credit card companies notified issuing banks, like Plaintiff and members of the proposed Class, of security breaches impacting company-issued debit and credit cards through various alerts.

71. As a result of the events detailed herein, Plaintiff and members of the proposed Class, to protect their customers and avoid fraud losses, cancelled the credit and debit cards they had issued. Plaintiff and members of the proposed Class reissued cards with new account numbers and magnetic strip information to customers. In January 2013, Plaintiff received a Compromised Account Management System (CAMS) Alert from Visa that approximately 1,100 debit cards had been compromised as a result of Defendant's data breach. CAMS is a secure system that allows acquirers, merchants, and law enforcement officers to upload compromised and stolen or recovered account numbers directly to Visa. Plaintiff has received a CAMS e-mail alert notifying Plaintiff of the compromised accounts.

72. As a result of Target's failure to safeguard customer information, to date, Plaintiff has been forced to cancel and reissue approximately 1,100 cards and incur related costs for notification and re-issuance of debit cards to its clients.

73. News reports indicate that the number of compromised cards requiring replacement is even higher for other issuing banks. For example, "JPMorgan Chase is replacing nearly two million cards as a result of the December security breach at Target."[23]

[23] http://www.wcpo.com/money/consumer/dont-waste-your-money/chase-replacing-cards-after-target-data-breach.

74. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the proposed Class. Moreover, as a result of the events detailed herein, Plaintiff and members of the proposed Class suffered losses resulting from Target's data breach related to: (a) reimbursement of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as purchasing and mailing new cards to its customers.

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

COUNT ONE: NEGLIGENT MISREPRESENTATION

76. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

77. In participating in the credit and debit card systems, Target falsely represented that it would comply with the Card Operating Regulations and would safeguard customer data to induce banks to act as issuing banks and provide their customers with credit and debit cards for use at Target stores.

78. Target's compliance with the Card Operating Regulations and safeguarding of customer data were material facts upon which Plaintiff and members of the proposed Class relied.

79. Target, which knew or should have known that it was not in compliance with the Card Operating Regulations and was not safeguarding customer data,

represented that it was so doing, which included a representation that it would not retain, store, or disclose the magnetic strip information and would maintain the confidentiality of the information.

80. Plaintiff and other members of the proposed Class agreed to act as an issuing bank for the debit and credit transactions expecting that large retail chains such as Target would comply with the Card Operating Regulations and would safeguard customer data. Plaintiff and members of the proposed Class relied upon and acted in reliance upon such representations by Target.

81. Target failed to exercise reasonable care in communicating the information that Plaintiff and members of the proposed Class relied upon.

82. Plaintiff and members of the proposed Class justifiably relied upon the false representations made by Target regarding the security and confidentiality of the credit and debit card information.

83. Plaintiff and members of the proposed Class have suffered damages as detailed herein as a result of Target's misrepresentations.

COUNT TWO: UNLAWFUL DECEPTIVE ACTS AND PRACTICES UNDER MINN. STAT. ANN. §325F.69 SUBD. 1

84. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

85. Target is engaged in trade or commerce in the State of Minnesota.

86. Upon information and belief, the Target computer systems that process and store information related to credit and debit card transactions on which customer data was

retained and from which customer data was improperly access were located in Minneapolis, Minnesota.

87. Plaintiff and members of the proposed Class are financial institutions engaged in trade or commerce.

88. Target's false representations to Plaintiff and members of the proposed Class regarding its compliance with the Card Operating Regulations and 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. Ann. §325F.69 Subd. 1. Target's actions in connection with its 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 Plaintiff and members of the putative Class.

89. The unfair and deceptive acts and practices described above were knowingly unfair and/or willful, and Plaintiff and members of the proposed Class have suffered damages as detailed herein.

COUNT THREE: VIOLATION OF THE GRAMM-LEACH-BLILEY ACT AS UNLAWFUL DECEPTIVE ACTS AND PRACTICES UNDER MINN. STAT. ANN. §325F.69 SUBD. 1

90. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

91. Defendant has a duty pursuant to the Gramm-Leach-Blilely Act, 15 U.S.C. §6801 *et seq.* and 16 C.F.R. §313 *et seq.*, not to misuse or inappropriately disclose

information received as a third party for the purpose of processing a transaction requested by a customer of its stores.

92. Pursuant to 16 C.F.R. §313.11(iii), third party recipients of financial data, such as Defendant, cannot "use" or "disclose" the information other than in "the ordinary course of business to carry out the activity covered by the exception under which [it] received the information."

93. Defendant was obligated under 16 C.F.R. §313.11 to only use and disclose customer financial information for the purposes for which it was disclosed, more specifically, to process the transaction.

94. Plaintiff and members of the proposed Class, in the course of business, placed the nonpublic personal information of their cardholder-customers onto the magnetic strip of their cards with the expectation that retail merchants, such as Defendant, would access that information only for the purpose of processing transactions that are initiated by that customer.

95. Target violated the Gramm-Leach-Blilely Act in that it improperly used and disclosed the information in violation of the Privacy Regulations by: (a) maintaining the data well beyond the permitted timeframe; and/or (b) allowing the data to be accessed by others for purposes unrelated to the processing of the credit or debit transaction.

96. The above violations constitute unfair and/or deceptive trade practices under Minn. Stat. Ann. §325F.69 Subd. 1.

97. Plaintiff and members of the proposed Class have suffered damages as detailed herein as a result of Target's unfair and deceptive trade practices.

98. The unfair and deceptive acts and practices described above were knowingly unfair and/or willful.

COUNT FOUR: VIOLATION OF MINN. STAT. ANN. §325E.64

99. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

100. Defendant had a duty under Minn. Stat. Ann. §325E.64 Subd. 2, to provide notification of the data breach to Plaintiff and members of the proposed Class. Specifically, this subdivision directs 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.

101. Minn. Stat. Ann. §325E.64 Subd. 3 holds Defendant liable for its data breach. Specifically, this subdivision provides that:

> 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.

102. Defendant breached the duties it owed to Plaintiff and members of the proposed Class under Minn. Stat. Ann. §325E.64 by virtue of its illegal conduct as alleged herein.

103. As a direct and proximate result of Defendant's breach of its duties under Minn. Stat. Ann. §325E.64, Plaintiff and members of the proposed Class have suffered substantial losses as detailed herein.

COUNT FIVE: NEGLIGENCE

104. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

105. Defendant owed a duty to Plaintiff and members of the proposed Class to use and exercise reasonable and due care in obtaining and retaining the personal and financial information of Plaintiff and members of the proposed Class and their customers.

106. Defendant owed a duty to Plaintiff and members of the proposed Class to provide adequate security to protect the personal and financial information of Plaintiff and members of the proposed Class and their customers.

107. Defendant breached its duties, allowed an unlawful intrusion into its computer system, failed to protect against such an intrusion, and allowed personal and financial information of Plaintiff and members of the proposed Class and their customers to be accessed by third parties.

108. Defendant 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.

109. As a direct and proximate result of Defendant's carelessness and negligent conduct, Plaintiff and members of the proposed Class have suffered substantial losses as detailed herein.

COUNT SIX: BREACH OF CONTRACT

110. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

111. Target had a contract with an acquiring bank that required Target to comply with the Card Operating Regulations.

112. As detailed herein, Plaintiff and members of the proposed Class were intended third party beneficiaries to the contract entered into by Target and the acquiring bank.

113. Target breached its obligations to Plaintiff and members of the proposed Class as third party beneficiaries of Target's contract with the acquiring bank.

114. As a direct and proximate result of Target's breach of contract, Plaintiff and members of the proposed Class have suffered losses as detailed herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Putnam Bank and members of the proposed Class seek damages against Defendant for the conduct detailed herein. Plaintiff demands judgment against Defendant as follows:

A. Certification of the Class under Fed. R. Civ. P. 23 and appointment of Plaintiff as representative of the Class and its counsel as lead Class counsel pursuant to Fed. R. Civ. P. 23(g);

B. Money damages;

C. Treble damages for willful and knowing violations of Minn. Stat. Ann. §325F.69 Subd. 1;

D. A finding that Target violated Minn. Stat. Ann. §325E.64 and an order enjoining Target from any further improper retention of customer data;

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

F. Costs;

G. Pre and post judgment interest; and

H. Such other and further relief as the Court deems just and equitable.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury on all issues so triable.

DATED: January 13, 2014

ZIMMERMAN REED, PLLP

/s/ Brian C. Gudmundson

Brian C. Gudmundson MN 336695
J. Gordon Rudd, Jr. MN 222082
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Tel: (612) 341-0400
Fax: (612) 341-0844
brian.gudmundson@zimmreed.com
gordon.rudd@zimmreed.com

Joseph P. Guglielmo
Joseph D. Cohen
SCOTT+SCOTT,
ATTORNEYS AT LAW, LLP
The Chrysler Building
405 Lexington Avenue, 40th Floor
New York, NY 10174
Tel.: (212) 223-6444
Fax: (212) 223-6334
jguglielmo@scott-scott.com
jcohen@scott-scott.com

David R. Scott
Stephen J. Teti
SCOTT+SCOTT,
ATTORNEYS AT LAW, LLP
156 South Main Street, P.O. Box 192
Colchester, CT 06415
Tel.: (860) 537-5537
Fax: (860) 537-4432
david.scott@scott-scott.com
steti@scott-scott.com

Counsel for Plaintiff