UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation This Document Relates to: All Financial Institutions Cases	MDL No. 14-2522 (PAM/JJK) **CONSOLIDATED CLASS ACTION COMPLAINT**

Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union, and First Federal Savings of Lorain, Individually and on behalf of a class of all similarly situated financial institutions in the United States, Plaintiffs, v. Target Corporation, Defendant.	JURY TRIAL DEMANDED

Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union, and First Federal Savings of Lorain (collectively, "Plaintiffs"), individually and on behalf of a class of all similarly situated financial institutions in the United States (the "FI Class"), assert the following claims against Target Corporation ("Target" or "Defendant") and in support thereof, state as follows:

SUMMARY OF ACTION

1. In late 2013, the sensitive financial and personal data of approximately 110 million shoppers was compromised as a result of Target's failure to adequately secure payment information on its systems. It was one of the largest data security breaches in United States history, yet Target's security protocols were so deficient that the breach continued for nearly three weeks while Target failed to even detect it.

2. The financial institutions that issued the debit and credit cards involved in Target's data breach have suffered substantial losses as a result of Target's failure to adequately protect its sensitive payment data. This includes, but is not limited to, sums associated with notifying customers of the data breach, reissuing debit and credit cards, reimbursing customers for fraudulent transactions, monitoring customer accounts to prevent fraudulent charges, addressing customer confusion and complaints, changing or canceling accounts, and the decrease or suspension of their customers' use of affected cards during the busiest shopping season of the year.

3. Plaintiffs seek to recover damages and equitable relief on behalf of themselves and all other similarly situated financial institutions in the United States.

JURISDICTION AND VENUE

4. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (1) the FI Class consists of more than 100 members; (2) the amount at issue is more than $5 million exclusive of interest and costs; and (3) minimal diversity exists as at least one plaintiff is a citizen of a different state than Defendant.

5. This Court has jurisdiction over Target because the company maintains its principal headquarters in Minnesota, regularly conducts business in Minnesota, and has sufficient minimum contacts in Minnesota. Target intentionally avails itself of this jurisdiction by marketing and selling products from Minnesota to millions of consumers nationwide (including in Minnesota).

6. Venue in this Court is appropriate pursuant to 28 U.S.C. § 1391(a) because Defendant's principal place of business is in this District and, furthermore, because a substantial part of the events, acts, or omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

7. Plaintiff Umpqua Bank is an Oregon state-chartered commercial bank headquartered in Roseburg, Oregon, with branches in Oregon, Idaho, Washington, California, and Nevada.

8. Plaintiff Mutual Bank is a Massachusetts state-chartered mutual bank headquartered in Whitman, Massachusetts, with branches in Massachusetts.

9. Plaintiff Village Bank is a Minnesota state-chartered, family-owned, community bank headquartered in St. Francis, Minnesota, with branches in Minnesota.

10. Plaintiff CSE Federal Credit Union is federally-chartered, member-owned and controlled financial cooperative headquartered in Lake Charles, Louisiana, with branches in Louisiana.

11. Plaintiff First Federal Savings of Lorain is a federally-chartered savings association headquartered in Lorain, Ohio, with branches in Ohio.

12. Plaintiffs are financial institutions that issue payment cards, including credit and debit cards, and/or perform, facilitate, or support card issuing services on behalf of their customers. Plaintiffs' customers used these payment cards to make purchases at Target stores during the period of the data breach in question.

13. Defendant Target is a Minnesota corporation with its principal place of business located at 1000 Nicollet Mall, Minneapolis, Minnesota 55403.

STATEMENT OF FACTS

14. Target is an international retail chain and the second largest retailer in the United States with 1,797 store locations. Between approximately November 15, 2013 and December 15, 2013, in one of the largest data breaches in history, the Company's computer systems were compromised and hackers obtained the personal and financial information of an estimated 110 million Target shoppers.

15. Information obtained by investigative journalists, security experts, government investigators, and by members of the U.S. Senate in hearings, shows the data breach easily could have been prevented as Target failed to take adequate and reasonable measures to ensure its data systems were protected, ignored *clear* warnings that intruders had breached its systems, and failed to take actions that could have thwarted the breach. Because of Target's numerous and preventable failures, Plaintiffs and the FI Class have suffered millions of dollars in damages.

16. Through its actions and inaction, Target has violated statutory and common laws designed to prevent such disasters, and those violations have caused Plaintiffs and the FI Class to suffer substantial damages.

Background on Electronic Debit and Credit Card Transactions

17. When a customer initiates a debit or credit card transaction at a retailer such as Target, as with virtually all credit or debit card transactions made on a credit card network, the process of completing that transaction involves four principal actors: (1) a merchant (such as Target), where the initial purchase is made; (2) an acquiring bank (which is typically a financial institution that contracts with the merchant to process its credit and debit card transactions); (3) a payment processor or card network (the system through which the transaction is conducted, *e.g.* Visa); and (4) the debit or credit card issuer (which is a financial institution like Plaintiffs and members of the FI Class, that issues credit cards and debit cards to consumers). In general, to process a purchase using a credit or debit card, a merchant first seeks authorization from the issuing bank for the transaction. In response, the issuing-bank informs the merchant whether it will approve or decline the transaction (generating the familiar "transaction approved" or "card declined" messages at the point of purchase). Assuming the transaction is approved, the merchant then electronically forwards the receipt directly to its acquiring bank. The acquiring bank then pays the merchant (*i.e.*, Target), forwards the final transaction data to the issuing bank, and the issuing bank reimburses the acquiring bank. The issuing bank (*i.e.*, Plaintiffs) then posts the charge to its customer's debit card or credit card account.

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

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

19. Similarly, the Payment Card Industry Data Security Standards ("PCI DSS") are a list of twelve information security requirements promulgated by the Payment Card Industry Security Standards Council. They apply to all organizations and environments where cardholder data is stored, processed, or transmitted and require merchants like Target to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies. In addition, the PCI DSS prohibited Target from retaining certain customer data. Specifically, the PCI DSS 2.0 requires merchants to adhere to the following rules:

Build and Maintain a Secure Network

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

- Restrict access to cardholder 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 for all personnel

20. In addition to the rules and regulations promulgated by the financial institutions that administer and oversee the credit and debit card networks used by Target, Target was subject to state legislation that was designed to ensure that Minnesota companies are vigilant in their efforts to prevent the type of data breach that occurred here. In 2007, in the wake of data breaches impacting other merchants across the United

States, Minnesota's legislature enacted one of the strongest data protection statutes in the country, which specifically codified some of the most pertinent provisions of the PCI DSS and was intended to address the very security deficiencies that led to the Target data breach.

21. In particular, Minnesota's Plastic Card Security Act, Minn. Stat. § 325E.64, imposes liability upon 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." 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."

22. Target was at all times fully cognizant of its data protection obligations in light of the existing web of regulations and laws requiring Target to take affirmative steps to protect the sensitive financial information entrusted to it by consumers and the financial institutions that participate in and administer credit and debit card processing systems.

23. Despite this, Target's treatment of the sensitive personal and financial information entrusted to it by its customers and Plaintiffs fell woefully short of its legal duties and obligations. Target failed to ensure that access to its data systems was reasonably guarded, and failed to acknowledge numerous warning signs and properly

utilize its own security systems that were put in place to detect and deter this exact type of attack.

Leading Up to the Breach: Target's Warnings

24. At the time of the breach, Target had specific notice of the potential attacks that could occur on its systems, and of the potential risks posed to the Company and to financial institutions such as Plaintiffs and the FI Class if it failed to adequately protect its systems.

25. As early as 2005, a notorious IT systems hacker, Albert Gonzalez, masterminded and implemented one of the largest coordinated data breaches in history, ultimately compromising more than 170 million credit and debit card accounts by infecting retailers' point of sale ("POS") terminals with malicious software (also known as malware) which transmitted, unencrypted, the financial data being processed by the POS machine to Gonzalez and his accomplices. In the end, Gonzalez and his cohorts were able to walk off with vast amounts of customer data from various retailers, *including customer data possessed by Target*.[1]

26. In May 2010, weaknesses in Target's POS systems were again exploited by hackers. As reported by the online retailer security newsletter, FierceRetailIT, 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")

[1] In fact, the Gonzalez data breach provided the impetus for passage of the Minnesota Plastic Card Security Act, Minn. Stat. § 325.64, which was designed to protect financial institutions in data breaches.

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."

27. Later, 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.

28. In January 2013, the Target security operations center, headquartered in Minneapolis, Minnesota, began the process of updating the Company's computer security systems, including its malware detection software. Target made this decision at a time when cyber-attacks on U.S. retailers were becoming more and more prevalent.

29. Several noteworthy reports published in 2013 put, or should have put, Target on notice of the increase in cyber-attacks on U.S. retailers. For instance, the U.S. government and several private research firms distributed industry-wide memos in 2013 on the emergence of new types of malicious computer code targeting retailers.

30. Visa Corporation also issued reports in April and August, 2013, alerting Target to attacks using RAM scraper malware, or memory parsing software, which enables cyber criminals to grab encrypted data by capturing it when it travels through the live memory of a computer. The reports detailed how the attacks were being launched and provided advice on thwarting them.

31. 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 only aware of the malware impacting the Windows operating system—*i.e.*, the exact operating systems Target used—and not any other operating system.

32. 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 securely delete the data"; and "assign strong passwords to your security solution to prevent application modification." Target did not implement these measures.

33. Target itself reported a "significant uptick" in malware trying to enter its computer systems throughout 2013.

34. In February 2013, Target hired FireEye, Incorporated ("FireEye"), a world renowned security software company, whose clients include the CIA and Pentagon, to update Target's computer security systems. FireEye's services included providing Target with state of the art malware detection tools, including a team of security specialists whose job was to monitor Target's computers around the clock, at a cost of $1.6 million to Target.

35. From March to May 2013, Target tested FireEye's security software, including its malware detection tools.

36. In June 2013, the FireEye tests were deemed successful and Target began to roll out the FireEye security software technology throughout its massive IT system. FireEye's security software was fully installed and fully functional prior to the date of the data breach at issue.

37. From June to August 2013, hackers in Eastern Europe began poking around the computer networks of various major U.S. retailers, including Target. The hackers were searching for routes that would take them deep into the retailer's corporate computer systems. The hackers' explorations eventually led them to a company named Fazio Mechanical Services ("Fazio"), a Pennsylvania refrigeration and HVAC contractor.

38. Fazio was a third-party vendor to Target, meaning it worked as a heating and air conditioning subcontractor at various Target stores in the U.S. As part of its subcontractor work, Target provided Fazio limited network credentials, which gave Fazio virtual access to certain parts of Target's computer network. Target gave Fazio the credentials to use for electronic billing, contract submission, and project management purposes.

39. Hackers were able to gather information on Target's vendors with a simple Google search. Target could have easily limited the amount of publicly available information that was available regarding its vendors, and could have also easily shared threat information with its suppliers and vendors and encouraged collaboration within its community of merchants.

40. Once the hackers learned that Fazio possessed credentials to Target's computer network, the hackers stole the credentials from Fazio sometime in September,

2013. The hackers stole the credentials by using a malware called Citadel. The process the hackers used is straightforward: hackers send the Citadel malware program to Fazio in an email, and when Fazio opens the email, Citadel attempts to steal all of Fazio's passwords. In this instance, Citadel was successful.

41. The hackers' theft of Fazio's credentials was made possible in large part to the grossly inadequate computer security systems in place at Fazio at the time of the theft. Specifically, Fazio's primary method of detecting malicious software – which is what the hackers used to steal the Target credentials – was the free version of a security program called Malwarebytes Anti-Malware ("MBAM"). This was problematic because MBAM is made for individual use and its license expressly prohibits corporate use, which is exactly how Fazio was using it at the time of the attack. Thus, with effectively no malicious software detection program in place at Fazio, the hackers easily stole Fazio's Target credentials. Here again, Target could have easily required adequate monitoring and anti-malware software for any vendors with access to Target's computer systems.

42. Armed with Fazio's Target credentials, the hackers began preparing for the next phase of their attack.

43. Around September 2013, numerous members of Target's security staff raised concerns about what they believed to be vulnerabilities in Target's payment card system. The vulnerabilities were due to updates being made to Target's cash registers, presumably in conjunction with the rolling out of the FireEye security software. The warnings went unheeded and Target officials ordered no further investigation.

44. On September 20, 2013, Target commissioned an audit, which certified that the Company was in compliance with all "payment industry requirements," including the Payment Card Industry Data Security Standards ("PCI DSS"), for protecting credit card data. In the aftermath of the data breach, however, Target admitted in its March 14, 2014 Form 10-K filed with the SEC:

> While an independent third-party assessor found the portion of our network that handles payment card data to be compliant with applicable data security standards in the fall of 2013, we expect the forensic investigator working on behalf of the payment card networks nonetheless to claim that we were not in compliance with those standards at the time of the Data Breach. We base that expectation on our understanding that, in cases like ours where prior to a data breach the entity suffering the breach had been found by an independent third-party assessor to be fully compliant with those standards, the network-approved forensic investigator nonetheless regularly claims that the breached entity was not in fact compliant with those standards. As a result, we believe it is probable that the payment card networks will make claims against us. We expect to dispute the payment card networks' anticipated claims, and we think it is probable that our disputes would lead to settlement negotiations consistent with the experience of other entities that have suffered similar payment card breaches.

Target's Unprecedented Security Breach

45. On November 15, 2013, the Target data breach began.

46. Armed with Fazio's Target credentials, the hackers easily logged onto Target's computer network. Once logged on, Fazio's credentials gave the hackers access to the billing, contract submission, and project management portions of Target's computer network only, and presumably nothing else. Target's computer network, however, was not properly segmented to ensure that its most sensitive parts were walled

off from the other parts of the network. The hackers exploited this gaping hole and uploaded their malware onto the most sensitive part of Target's computer system – its customer payments and personal data network.

47. The hole that left Target exposed to the hackers is called a "segmentation issue," which is a situation where computer systems within a network that should not be connected for security reasons are in fact connected. According to industry experts, there should never be a route between a network for an outside contractor (such as Fazio) and the network for payment data. In Target's case, however, there was, and the hackers found it and exploited it.

48. Once inside Target's customer payments and personal data network, the hackers uploaded their card-stealing malicious software onto a small number of cash registers within Target stores. During this time, the hackers tested their point-of-sale malware to ensure it was working as designed. To prevent this, Target could have required two-factor authentication for its vendors. Two-factor authentication includes a regular password system (like the one the hackers stole from Fazio) augmented by a second step, such as providing a code sent to the vendor's mobile phone or answering extra security questions (something the hackers did not possess).

49. On November 30, 2013, the hackers installed their card-stealing malware onto a majority of Target's in-store cash registers via remote upload over the Target network. The hackers also began to actively collect card records from live customer transactions. The way the malware worked was simple: when a customer went to any in-store Target cash register to pay for an item and swiped his or her card, the malware

stepped in and captured the shopper's card number and other sensitive financial information.

50. Also on or about November 30, 2013, the hackers installed exfiltration malware – a program that took the stolen information and moved it from Target's computer systems to the hackers' computer systems after several days. FireEye, Target's new security software provider, spotted the hackers while they were uploading the malware and alerted Target's security team about the suspicious activity. Target's security team took no action. Had Target immediately stepped in once FireEye alerted the Company to these suspicious activities, the hackers' plan would have been completely foiled.

51. According to a report from the U.S. Senate, Target could have blocked the effect of the hackers' malware on its servers by following up on the several alerts that FireEye triggered at the time of the malware delivery. Target could have also avoided the breach by paying greater attention to industry and government intelligence analyses, as these analyses included recommendations for reducing the risk of a successful attack. Finally, Target could also have taken action to address concerns voiced by its security staff regarding vulnerabilities on the Company's cash registers.

52. According to the U.S. Senate report, Target could have also avoided the data breach by taking two security measures called for in the PCI-DSS 2.0, the version of the PCI-DSS at the time of the breach. First, Target could have taken the protective step of eliminating unneeded default accounts, which is what the hackers used to gain access to the most sensitive parts of Target's network. Second, Target could have required

vendors to more closely monitor the integrity of their critical system files. This requirement would have put Fazio on notice that hackers had stolen its Target credentials.

53. Also on November 30, 2013, at approximately the same time that FireEye, Target's malware detection system, was spotting suspicious activity on Target's computer network, Target's antivirus system, Symantec Endpoint Protection ("SEP"), also identified the same type of suspicious behavior. Target again took no action pursuant to SEP's warning, just as it took no action in response to FireEye's warnings. Target's inaction allowed the entirely preventable data breach to continue.

54. On December 2, 2013, Target received the *exact same* alert from FireEye that it had received on November 30, 2013. Yet again, Target failed to respond to the alert, thereby missing its third opportunity to prevent the data breach from ever occurring.

55. After three missed opportunities by Target to prevent the data breach, the hackers began the process of actually stealing Target customers' card information from Target's systems.

56. From December 2-15, 2013, with the malware installed on Target's cash registers and the extraction software on Target's servers, the hackers collected customers' card information, including in real time each time customers swiped their card at a Target store. The data from each register was then automatically sent to one of three staging points – secret places installed on *Target's own computer network* where the hackers temporarily stored the data before sending it offshore. The out of place data sat undetected on Target's own network for six days to avoid setting off any internal alarms within Target's network. After six days, the data was laundered through a variety of

sham computer servers, eventually ending up at its final destination – a server in Russia belonging to the hackers.

57. The hackers repeated this process for almost two weeks completely unmolested.

58. According to the U.S. Senate report, Target could have disrupted the hackers at this point of the scheme where they were transferring the data by erecting strong firewalls between Target's internal systems and the outside Internet to help disrupt the hackers' ability to command and control the company's computer network as easily as it did. Target could have also filtered or blocked certain Internet connections commonly used from command and control hacking.

59. The U.S. Senate report also determined Target could have created a list of approved servers to which Target's network was allowed to upload. Specifically, the list could have dismissed connections between Target's networks and Russian-based Internet servers, which, given that Russia was the end location for the stolen data and a hot bed of fraudulent hacker activity, would have prevented the breach. Furthermore, Target's FireEye software did detect the data exfiltration malware, yet Target did nothing in response to the report. Again, acting on this information could have stopped the exfiltration.

60. On December 11, 2013, a currently unidentified individual within Target first detected the malware used in the breach and submitted it to Virustotal. Virustotal is a company that produces reports about suspicious files submitted by users. The submission was attributable to someone within Target because the malware was widely

thought to be custom-made specifically for the Target intrusion. Thus, it stands to reason that the person who found and submitted the malware must work for Target. Despite being on notice of the malware on this date, Target continued to do nothing and allowed the breach to continue for four more days.

61. Information stolen from Target's systems quickly flooded the black market, with the hackers quickly trying to sell the valuable information they had stolen. According to The New York Times:

> 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.

62. Throughout the month of December, the hackers uploaded new stolen cards to a card shop website (an illegal website where stolen credit and debit card information is sold.) Some stolen cards were lumped together under the moniker "Tortuga," which was to inform purchasers that the cards were unused, high-quality, and worth their purchasing price.

63. On December 20, 2013, an illegal card shop website announced the availability of a new database of stolen credit/debit cards called "Barbarossa"—which consisted of more than 330,000 debit and credit cards issued by banks in Europe, Asia, Latin America, and Canada. Brian Krebs, a journalist and cybersecurity expert, 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 database also were used at Target during the breach timeframe*." The cards for sale in the Barbarossa database vary widely in price from $23.62 per card to as high as $135 per card.

64. On December 12, 2013, the bank JP Morgan Chase alerted some credit card companies that fraudulent charges were showing up on credit cards that were all recently used at Target stores in the U.S.

65. Also on December 12, 2013, the U.S. Justice Department contacted Target to alert the Company about the breach. Rather than immediately springing into action to rectify its systems and notify the public, Target scrutinized the Justice Department's information for three days to try and confirm the veracity of the U.S. officials' statements, thereby allowing the data breach to continue for an additional three days.

66. Finally, on December 15, 2013, Target began purging its computer system of the hackers' malware, and after two weeks of uninterrupted data collection (the groundwork for which had been laid weeks before that), the Target data breach finally came to an end.

67. As Target has admitted, the Company had multiple opportunities to identify and prevent the attack on its data systems, but key personnel at Target remained unaware

or unconcerned about what had occurred until days after investigations by the Department of Justice and computer security experts identified the massive breach.

The Aftermath of Target's Data Breach

68. Once informed of the breach on December 12, 2013, Target sat on the information for seven days, rather than immediately notifying the public of the monstrous breach of millions of credit and debit cards that were already flooding the black market.[2] When Target finally did acknowledge the data breach publicly on December 19, 2013, it was only because someone else had already broken the news.

69. Brian Krebs is credited with "breaking" the news of the Target data breach. Sometime prior to December 19, Krebs spoke with a fraud analyst at a major bank who informed Krebs that his team had independently confirmed that Target had been breached. The analyst confirmed the breach after buying a large number of the bank's card accounts from a black market card site run by the Target hackers.

70. With this information and information from other reliable sources, Krebs broke the Target data breach story on his blog, *Krebs on Security*, on December 18, 2013. That day, Krebs began leaving voice messages for Target's public affairs department asking about the data breach. Krebs specifically mentioned his conversations with the fraud analyst and that the common spending link on the stolen cards was Target. Target ignored Krebs' requests for comment.

[2] In February 2014, John Mulligan, then Target's Executive Vice President and CFO, testified that Target learned of the data breach on December 12, 2013, that Target confirmed the data breach on December 15, 2013, and that Target informed the general public of the data breach on December 19, 2013.

71. On December 19, 2013, seven days after learning of the breach, Target publicly disclosed for the first time that its payment card data had been compromised, and that "customer name, credit or debit card number, and the card's expiration date and CVV" (in other words, the full magnetic stripe data embedded in debit and credit cards that Target was prohibited by law from retaining) of approximately 40 million customers had been stolen.

72. Despite that admission, Target attempted to downplay the significance of the breach to avoid jeopardizing holiday sales, reassuring customers that there was "no indication that debit card PINs were impacted." Indeed, Target claimed that it was "confident that PIN numbers are safe and secure" and thieves could not "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's then-CEO Gregg Steinhafel explaining that the discount was in the "spirit" of "we're in this together."

73. Contrary to Target's assurances, one week later, on December 27, 2013 (two days *after* the Christmas holiday), Target admitted that, in fact, "PIN data was removed" from Target's systems.

74. On January 10, 2014, Target announced that the breach was orders of magnitude greater than it originally reported, admitting that up to 110 million people were affected by the breach. Target admitted the new subset of victims included customers who may not have shopped at Target during the holiday period previously mentioned in Target's first public press release. Target noted that while there may be

some overlap between the two groups (the initial group and the newly identified group) it did not know the extent of the overlap.

75. In addition to increasing its estimate of the sheer volume of the breach, Target also disclosed that the nature of the data stolen was much broader, and much worse, than originally thought, admitting 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." Target further conceded that the 110 million affected by the breach included customers *who did not even swipe* their debit or credit cards at a Target store in the November to December period during which Target originally claimed customer data had been compromised – confirming that Target had improperly retained customer data (potentially for many months) that the hackers also extracted as a result of the breach.

The Continuing Fallout from Target's Internal Policies and the Data Breach

76. Despite receiving multiple warnings from government and industry security experts, its own employees, and even its own computer security system, Target took no actions to protect its customers' sensitive data. Target's unreasonable data policies have cost Plaintiffs and the FI Class millions of dollars of damages.

77. An investigation by *Bloomberg Businessweek*, citing conversations with "10 former Target employees familiar with the company's data security operation, as well as eight people with specific knowledge of the hack and its aftermath," found, and Plaintiffs allege, that FireEye's malware detection program "worked beautifully. But

then, Target stood by as 40 million credit card numbers—and 70 million addresses, phone numbers, and other pieces of personal information—gushed out of its mainframes." As *Bloomberg* further stated,

> In testimony before Congress, Target has said that it was only after the U.S. Department of Justice notified the retailer about the breach in mid-December that company investigators went back to figure out what happened. What it hasn't publicly revealed: Poring over computer logs, Target found FireEye's alerts from Nov. 30 and more from Dec. 2, when hackers installed yet another version of the malware. Not only should those alarms have been impossible to miss, they went off early enough that the hackers hadn't begun transmitting the stolen card data out of Target's network. Had the company's security team responded when it was supposed to, the theft that has since engulfed Target, touched as many as one in three American consumers, and led to an international manhunt for the hackers never would have happened at all.
>
> * * *
>
> On Nov. 30, according to a person who has consulted on Target's investigation but is not authorized to speak on the record, the hackers deployed their custom-made code, triggering a FireEye alert that indicated unfamiliar malware: "malware.binary." Details soon followed, including addresses for the servers where the hackers wanted their stolen data to be sent. As the hackers inserted more versions of the same malware (they may have used as many as five, security researchers say), the security system sent out more alerts, each the most urgent on FireEye's graded scale, says the person who has consulted on Target's probe.
>
> The breach could have been stopped there without human intervention. The system has an option to automatically delete malware as it's detected. But according to two people who audited FireEye's performance after the breach, Target's security team turned that function off.

78. Bloomberg's report was later substantiated by an investigation, analysis, and report conducted by the United States Senate's Committee on Commerce, Science and Transportation. After conducting what is termed a "Kill Chain analysis"[3] the Senate report concluded the following:

> *This analysis suggests that Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach.* Key points at which Target apparently failed to detect and stop the attack include, but are not limited to, the following:
>
> - Target gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted information security practices. The vendor's weak security allowed the attackers to gain a foothold in Target's network.
>
> - *Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system*.
>
> - Attackers who infiltrated Target's network with a vendor credential appear to have successfully moved from less sensitive areas of Target's network to areas storing consumer data, *suggesting that Target failed to properly isolate its most sensitive network assets*.
>
> - *Target appears to have failed to respond to multiple warnings from the company's anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network.*

[3] The fundamental premise of kill chain security is that hackers must proceed through seven steps to plan and execute an attack – these steps are called the "kill chain." While the hackers must complete all of these steps to execute a successful attack, the company has to stop the hackers from completing just one of these steps to prevent the attack. Put simply, a company has seven different opportunities along the kill chain to prevent the attack from occurring.

79. These findings were consistent with other news reports, virtually all of which concluded that the breach of Target's data systems was a result of both inadequate security and a total failure to respond. For example, *The New York Times* reported that Target's security systems were so "astonishingly" open that hackers were able to wander freely throughout Target's computer systems, downloading customer information at will. The same article went on to report that interviews with "people knowledgeable about the investigation, cybersecurity and credit experts" confirmed that Target's "system was particularly vulnerable to attack" and, according to experts, was so "remarkably open" that hackers were able to "wander from system to system, scooping up batches of information."

80. Publically available information indicates the massive scope of the data breach, and Target's cavalier attitude to the sensitive data entrusted to it, was endemic to the Company's culture. As profiled in a 2012 article in *The New York Times*:

> *For decades, Target has collected vast amounts of data on every person who regularly walks into one of its stores*. Whenever possible, Target assigns each shopper a unique code — known internally as the Guest ID number — that keeps tabs on everything they buy. "*If you use a credit card* or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail we've sent you or visit our Web site, *we'll record it and link it to your Guest ID*," [Target executive Andrew] Pole said. "*We want to know everything we can*."

81. Indeed, Target's collection, storage and analysis of customer data is so extensive that, as *The New York Times* reported, the Company developed a program that used the customer data it collected to predict when a customer might be pregnant in order

to direct advertisements for baby products at that customer, and to influence shopping behavior. As reported:

> One Target employee I spoke to provided a hypothetical example. Take a fictional Target shopper named Jenny Ward, who is 23, lives in Atlanta and in March bought cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug. There's, say, an 87 percent chance that she's pregnant and that her delivery date is sometime in late August. What's more, because of the data attached to her Guest ID number, Target knows how to trigger Jenny's habits. They know that if she receives a coupon via e-mail, it will most likely cue her to buy online. *They know that if she receives an ad in the mail on Friday, she frequently uses it on a weekend trip to the store.*

82. Target has also admitted that it has *kept sensitive customer financial data for 60 to 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 Transactions Act of 2003 ("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—of the credit card or debit card and the expiration date and the cardholder's name, in its computer system." As explained by John Kindervag, an analyst from Forrester Research and a leading security expert, "[Target] is a breach that should've never happened . . . *The fact that three-digit CVV security codes were compromised shows they were being stored . . . .*" (Emphasis added.)

83. Target's public acknowledgement that it was failing to adhere to industry standards regarding the retention and use of credit and debit card information not only confirms that Target failed to take measures that led to its vulnerability, but also that those failures may have put hackers on notice that one of the largest retailers in the world was carefully cataloging and keeping the credit and debit card information of all of its customers.

84. On March 5, 2014, Beth Jacob, Target's Chief Information Officer and the highest-ranking technology executive at Target, resigned in the aftermath of the Target data breach and revelations about the Company's data collection and security practices. On May 5, 2014, CEO Gregg Steinhafel also resigned.

The Fallout Continues for Financial Institutions and Their Customers

85. Beth Givens, who runs the San Diego-based Privacy Rights Clearinghouse, has stated, and Plaintiffs allege that, the biggest threat is for people who shopped at Target using debit cards, which withdraw money directly from users' checking accounts. As noted by Givens, laws are less protective of debit cards, and possession of a stolen PIN number could mean unauthorized access at an ATM: "[i]f you used a debit card at Target, I would recommend that you cancel it." With a debit card you risk having your checking account wiped out. It will certainly be replenished, but it may take several weeks." Plaintiffs and the FI Class are primarily responsible for paying for card replacement and for reimbursing fraudulent charges. While a consumer may ultimately be protected from these costs, Plaintiffs and the FI Class are not.

86. Target's completely avoidable data breach inflicted significant financial damage upon Plaintiffs and the FI Class, who had to act immediately to mitigate present credit and debit card fraud, while simultaneously taking steps to prevent future fraud. Plaintiffs and the FI Class were forced to dedicate significant capital and human resources to the task of addressing the breach including, but not limited to, reissuing cards, changing or closing accounts, notifying customers of the breach of their cards, investigating claims of fraudulent activity, refunding customers for fraudulent charges, and increasing fraud monitoring on potentially impacted accounts. Plaintiffs and the FI Class also lost interest and transaction fees (including interchange fees) as a result of decreased, or ceased, card usage in the wake of the Target data breach.

87. The costs suffered by Plaintiffs and the FI Class as a result of Target's data breach will almost certainly increase. Alphonse R. Pascual, of Javelin Strategy & Research, has predicted that stolen Target 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*." In fact, it has been estimated that the costs to banks and retailers caused by Target's breach could eventually exceed $18 billion.

CLASS ACTION ALLEGATIONS

88. Plaintiffs bring this action on behalf of themselves and all other financial institutions similarly situated and, accordingly, allege all claims herein on a common, class-wide, basis, pursuant to Fed. R. Civ. P. 23.

89. The FI Class is defined as follows:

> Financial institutions—including, but not limited to, banks and credit unions—in the United States (including its Territories and the District of Columbia) that issue payment cards, including credit and debit cards, or perform, facilitate, or support card issuing services, whose customers made purchases from Target stores from November 1, 2013 to December 19, 2013 (the "FI Class").

90. Excluded from the FI Class are Target Corporation and any of its parents, affiliates, or subsidiaries as well as any successors in interest or assigns of Target.

91. All Plaintiffs are members of the FI Class, as defined above.

92. The members of the FI Class are readily ascertainable and Target likely has access to addresses and other contact information that may be used for providing notice to FI Class members.

93. The members of the FI Class are so numerous that joinder of all members would be impracticable. Upon information and belief, the data breach at issue—which affected up to 110 million credit and debit cards—impacted thousands of financial institutions spread across virtually every geographic region of the United States.

94. There are substantial questions of law and fact common to the FI Class that predominate over questions affecting only individual FI Class members including, but not limited to, the following:

a. Whether Target owed a duty to Plaintiffs and the FI Class to adequately protect the personal and financial information of its shoppers;

b. Whether Target breached its duty to protect the personal and financial information of its shoppers by failing to provide adequate security;

c. Whether Target's conduct (or lack thereof) was the direct and proximate cause of the breach of its systems, which resulted in the loss of millions of consumers' personal and financial data;

d. Whether Target improperly retained sales transaction data beyond the period of time permitted by law;

e. Whether Target violated Minn. Stat. § 325E.64;

f. Whether Target negligently failed to inform Plaintiffs and the FI Class regarding the vulnerabilities of its data protection systems, measures, and practices;

g. Whether Plaintiffs and the FI Class suffered financial injury as a result of Defendant's conduct (or lack thereof);

h. Whether Plaintiffs and the FI Class are entitled to injunctive relief; and

i. What is the appropriate measure of damages sustained by Plaintiffs and the FI Class.

95. Plaintiffs' claims are typical of the FI Class. The same events and conduct that give rise to Plaintiffs' claims are identical to those that give rise to the claims of every other FI Class member because each Plaintiff is a financial institution that has

suffered harm as a direct and proximate cause of the same, specific Target data breach described herein.

96. Plaintiffs' interests are consistent with and not antagonistic to those of the other members of the FI Class.

97. Plaintiffs will fairly and adequately represent the interests of the FI Class. Plaintiffs have retained (and the Court has appointed) counsel who are experienced and qualified in prosecuting class action cases similar to this one.

98. Neither Plaintiffs nor their attorneys have any interest contrary to or conflicting with those of other members of the FI Class.

99. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the other FI Class members' claims is economically unfeasible and procedurally impracticable. Litigating the claims of the FI Class together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and unnecessary expense to the parties and the courts.

COUNT ONE
(Negligence)

100. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

101. Target owed a duty to Plaintiffs and the FI Class to use and exercise reasonable and due care in obtaining, retaining, securing, and deleting the personal and financial information of customers who used credit and debit cards issued by Plaintiffs and the FI Class to make purchases at Target stores.

102. Target owed a duty to Plaintiffs and the FI Class to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of customers who used credit and debit cards issued by Plaintiffs and the FI Class to make purchases at Target stores.

103. Target owed a duty of care to Plaintiffs and the FI Class because they were a foreseeable and probable victim of any inadequate data security practices. Target solicited, gathered, and stored the sensitive financial data provided by Plaintiffs and the FI Class to facilitate sales transactions with shoppers. Target knew it inadequately safeguarded this information on its computer systems and that sophisticated hackers routinely attempted to access this valuable data without authorization. Target knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiffs and the FI Class, and Target was therefore charged with a duty to adequately protect this critically sensitive information.

104. Target maintained a special relationship with Plaintiffs and the FI Class. The FI Class entrusted Target with the personal and financial information of customers using credit and debit cards issued by Plaintiffs on the premise that Target would safeguard this information, and Target was in a position to protect against the harm suffered by the FI Class as a result of the data security breach.

105. In light of its special relationship with Plaintiffs and the FI Class, Target knew, or should have known, of the risks inherent in collecting and storing the personal

and financial information of shoppers using credit and debit cards issued by Plaintiffs and the FI Class, and the importance of providing adequate security of that information.

106. Target's own conduct also created a foreseeable risk of harm to the FI Class. Target's misconduct included, but was not limited to, its hiring of a vendor that did not follow broadly accepted security practices, and permitting that vendor credentials that could be used to access Target's most sensitive systems. Target's misconduct also included its decision not to comply with industry standards for the safekeeping and maintenance of customers' personal and financial information.

107. Target breached the duties it owed to Plaintiffs and the FI Class by failing to exercise reasonable care and implement adequate security protocols—including protocols required by industry rules—sufficient to protect the personal and financial information of customers using credit and debit cards issued by Plaintiffs and the FI Class.

108. Target breached the duties it owed to Plaintiffs and the FI Class by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

109. Target breached the duties it owed to Plaintiffs and the FI Class by failing to properly maintain the sensitive personal and financial information of customers using credit and debit cards issued by Plaintiffs and the FI Class. Given the risk involved and the amount of data at issue, Target's breach of its duty was entirely unreasonable.

110. Target also knew Plaintiffs and the FI Class were foreseeable victims of a data breach of its systems because of specific laws and statutes that required Target to

reasonably safeguard sensitive payment information or be held liable in the event of a data breach. This includes Minn. Stat. § 325E.64, separately alleged below, which was passed in Target's own home state of Minnesota, and which exists expressly because financial institutions are foreseeable victims of a data breach of this type.

111. As a direct and proximate result of Target's negligent conduct, Plaintiffs and the FI Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT TWO
(Minnesota Plastic Card Security Act – Minn. Stat. § 325E.64)

112. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

113. Minn. Stat. § 325.64 is a Minnesota statute that specifically acknowledges Target's duty to safeguard transaction payment information owed to financial institutions such as Plaintiffs and the FI Class.

114. Minn. Stat. § 325E.64, subd. 2, imposed a duty upon Target not to retain payment information from sales transactions for longer than 48 hours. The statute specifically requires 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.

115. Minn. Stat. § 325E.64, subd. 3 details a merchant's responsibilities should it breach the duties imposed by the statute, and then subsequently suffer a data breach. 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.

116. Target "conducts business" in the State of Minnesota.

117. Target regularly accepts "access devices" (debit/credit cards) for the purpose of conducting its business.

118. Target violated Minn. Stat. § 325E.64 by retaining the card security code data, the PIN verification code number, and/or the full contents of Target customers' magnetic stripe data in violation of the statute.

119. There was a breach of the security of Target's system.

120. As a direct and proximate result of Target's violation of Minn. Stat. § 325E.64, Plaintiffs and the FI Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT THREE
(Negligence Per Se – Minn. Stat. § 325E.64)

121. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

122. As described above, Target violated Minn. Stat. § 325E.64 by improperly retaining the card security code data, the PIN verification code number, and/or the full contents of Target customers' magnetic stripe data from credit and debit cards issued by Plaintiffs and the FI Class.

123. Plaintiffs and the FI Class suffered harm, including, but not limited to, costs for reissuing credit/debit cards, changing or closing accounts, opening or reopening accounts, refunding or crediting cardholder accounts in response to fraudulent charges,

issuing notice to potentially effected cardholders, and other actions necessary to rectify, prevent and/or mitigate fraud as a result of Target's violation.

124. Plaintiffs and the FI Class are entities that the Minnesota legislature intended to be protected by Minnesota's Plastic Card Security Act, Minn. Stat. § 325E.64.

125. The injuries suffered by Plaintiffs and the FI Class were directly and proximately caused by Target's violation of Minnesota's Plastic Card Security Act, Minn. Stat. § 325E.64.

126. Target's violation of the Minnesota's Plastic Card Security Act, Minn. Stat. § 325E.64, thus constitutes negligence *per se* and Plaintiffs and the FI Class are entitled to recover damages in an amount to be proven at trial.

COUNT FOUR
(Negligent Misrepresentation by Omission)

127. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

128. Through its Privacy Policy and other actions and representations, Target held itself out to Plaintiffs and the FI Class as possessing and maintaining adequate data security measures and systems that were sufficient to protect the personal and financial information of shoppers using credit and debit cards issued by Plaintiffs and the FI Class.

129. Target further represented that it would secure and protect the personal and financial information of shoppers using credit and debit cards issued by Plaintiffs and the FI Class by agreeing to comply with both Card Operating Regulations and the PCI DSS.

130. Target knew or should have known that it was not in compliance with the representations made in its Privacy Policy, and the requirements of Card Operating Regulations and the PCI DSS.

131. Target knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to Plaintiffs and the FI Class.

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

133. Target also failed to exercise reasonable care when it failed to timely communicate information concerning the data breach that it knew, or should have known, compromised the personal and financial information of customers using credit and debit cards issued by Plaintiffs and the FI Class.

134. As a direct and proximate result of Target's negligent misrepresentations by omission, Plaintiffs and the FI Class have suffered injury and are entitled to damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of themselves and the FI Class, respectfully request that the Court enter judgment in their favor as follows:

a. certifying the FI Class under Fed. R. Civ. P. 23 and appointing Plaintiffs and their counsel to represent the Class pursuant to Fed. R. Civ. P. 23(g);

b. awarding Plaintiffs and the FI Class monetary damages as allowable by law;

c. awarding Plaintiffs and the FI Class appropriate equitable relief;

d. awarding Plaintiffs and the FI Class pre-judgment and post-judgment interest;

e. awarding Plaintiffs and the FI Class reasonable attorneys' fees and costs as allowable by law; and

f. awarding all such further relief as allowable by law.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and the FI Class, demand a trial by jury on all issues so triable.

Dated: August 1, 2014

ZIMMERMAN REED, PLLP

By: /s/ Charles S. Zimmerman
Charles S. Zimmerman (MN 120054)
J. Gordon Rudd, Jr. (MN 222082)
Brian C. Gudmundson (MN 336695)
1100 IDS Center
80 South 8th St.
Minneapolis, MN 55402
Telephone: (612) 341-0400
charles.zimmerman@zimmreed.com
gordon.rudd@zimmreed.com
brian.gudmundson@zimmreed.com

Lead Counsel for Financial Institution Plaintiffs

CHESTNUT CAMBRONNE PA
Karl L. Cambronne, #14321
Jeffrey D. Bores, #227699
Bryan L. Bleichner, #0326689
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Telephone: (612) 339-7300
kcambronne@chestnutcambronne.com
jbores@chestnutcambronne.com
bbleichner@chestnutcambronne.com

Coordinating Lead Counsel for Plaintiffs

REINHARDT WENDORF & BLANCHFIELD
Garrett Blanchfield
E-1250 First National Bank Building
332 Minnesota Street
St. Paul, MN 55101
Telephone: (651) 287-2100
g.blanchfield@rwblawfirm.com

Coordinating Liaison Counsel for Plaintiffs

LOCKRIDGE GRINDAL NAUEN P.L.L.P.
Karen Hanson Riebel
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
khriebel@locklaw.com

Liaison Counsel for Financial Institution Plaintiffs

LEVIN, FISHBEIN, SEDRAN & BERMAN
Howard J. Sedran
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
hsedran@lfsblaw.com

BARRETT LAW GROUP, P.A.
Don Barrett
404 Court Square North
PO Box 927
Lexington, MS 39092
Telephone: (662) 834-9168
dbarrett@barrettlawgroup.com

KESSLER TOPAZ MELTZER & CHECK LLP
Naumon A. Amjed
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
namjed@ktmc.com

CARLSON LYNCH LTD
Gary F. Lynch
115 Federal Street, Suite 210
Pittsburgh, PA 15212
Telephone: (412) 322-9243
glynch@carlsonlynch.com

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

BEASLEY, ALLEN, CROW, METHVIN, PORTIS MILES, P.C.
W. Daniel Miles, III.
272 Commerce Street
PO Box 4160
Montgomery, AL 36103-4160
Telephone: (334) 269-2343
dee.miles@beasleyallen.com

HAUSFELD LLP
James J. Pizzirusso
1700 K Street NW, Suite 650
Washington D.C. 20006
Telehone: (202) 540-7200
jpizzirusso@hausfeldllp.com

Plaintiffs' Leadership Committee

CARNEY BATES & PULLIAM, PLLC
Hank Bates
11311 Arcade Drive
Little Rock, AR 72212
Telephone: 501.312.8500
hbates@cbplaw.com

Counsel for Umpqua Bank