UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UMPQUA BANK, on behalf of itself and all others similarly situated, Plaintiff, v. TARGET CORPORATION, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Comes the Plaintiff Umpqua Bank ("Plaintiff"), acting individually and on behalf of all other persons similarly situated, and for its Complaint and demand for jury trial states and alleges as follows:

INTRODUCTION

1. This case arises from one of the largest data breaches in history, in which criminals obtained sensitive financial and personal data from the accounts of up to 110 million Target Corporation ("Target," "Defendant," or "the Company") customers. Specifically, starting on or about November 27, 2013, and continuing until on or about December 15, 2013, unknown third parties obtained customer records, held by Target, of as many as 110 million individuals. Such data included customer names, credit and debit card numbers, the card expiration dates, card verification values ("CVVs"), PIN numbers, mailing addresses, phone numbers, and email addresses.

2. As alleged herein, this data breach was made possible only because Target – the second largest retailer in the nation – failed to maintain adequate security

protocols despite having suffered two nearly identical data breaches in the preceding years and being warned multiple times – once in April of 2013 and again in August of 2013 – of the *precise* threat that led to the ultimate compromise.

3. Indeed, as details of the data breach emerge, security experts profess bewilderment by the level of negligence exhibited by Defendant in maintaining the security of highly sensitive consumer financial data. Reports proliferate of Target's "astonishingly" vulnerable security systems, which "lack[] the virtual walls and motion detectors found [as a matter of course] in secure networks."[1]

4. In an effort to prevent a mass exodus of customers, Target CEO Gregg Steinhafel took pains to assure consumers that "they will not be held financially responsible for any credit and debit card fraud."[2] However, what Steinhafel's statement omits is the fact that it is the nation's financial institutions – and not Target – ensuring that this is the case. To date, Plaintiff, along with all other financial institutions making up the proposed Class, has incurred costs associated with protecting its customers' accounts, particularly in the form of providing notice to customers, reissuing payment cards, and refunding fraudulent charges associated with bank accounts of customers who used their cards at Target during the period of the latest data breach. A recent study conducted by the Consumer Bankers Association and the Credit Union National

[1] Elizabeth A. Harris, Nicole Perlroth, Nathaniel Popper and Hilary Stout., "A Sneaky Path into Target Customers' Wallets," *N.Y. Times* (Jan. 17, 2014) (available at http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html).

[2] Gregg Steinhafel, "A Message From CEO Gregg Steinhafel About Target's Payment Card Issues," (Dec. 20, 2013) (available at http://pressroom.target.com/news/a-message-from-ceo-gregg-steinhafel-about-targets-payment-card-issues).

Association estimates the costs of card replacements, alone, to ultimately rest around $200 million.[3] This figure does not, however, include costs associated with reimbursing customers for fraudulent charges, or costs associated with lost transactional opportunities arising from decreasing consumer confidence in the security of payment cards.

5. Plaintiff brings this class action on behalf of all financial institutions, including banks and credit unions, in the United States that have had the confidential financial data associated with their customers' accounts – including but not limited to customer names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs – compromised as a result of the data breach at Target stores from the period beginning on or about November 27, 2013, and ending on or about December 15, 2013.

6. Plaintiff additionally seeks to represent a Sub-Class of all financial institutions, including banks and credit unions, in the State of Oregon that have had the confidential financial data associated with their customers' accounts – including but not limited to customer names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs – compromised as a result of the data breach at Target stores from the period beginning on or about November 27, 2013, and ending on or about December 15, 2013.

[3] Juan Carlos Rodriguez, "Target Hack Costs Over $200M for Banks, Groups Say," *Law360* (Feb. 20, 2014) (available at http://www.law360.com/privacy/articles/511396?nl_pk=9e2e8a6f-f702-466f-84ee-2a41d5618600&utm_source=newsletter&utm_medium=email&utm_campaign=privacy).

PARTIES

7. Plaintiff is a state-chartered commercial bank headquartered in Roseburg, Oregon. It provides banking services for both individual and business customers throughout the States of Oregon, Washington, California, and Nevada. Plaintiff's customers had their personal and financial information stolen as a result of a massive data breach occurring throughout the country at the stores of Defendant Target Corporation, from approximately November 27, 2013, until December 15, 2013. As a result of this theft, Plaintiff experienced losses, including, without limitation, the cost of notifying customers and reissuing debit cards in order to prevent future fraudulent activity, as well as refunding fraudulent charges associated with customer accounts affected by Target's data breach.

8. Defendant Target Corporation is an American corporation, incorporated under the laws of Minnesota and headquartered in Minneapolis, Minnesota.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over this class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs, and is a class action in which some Members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A).

10. Venue properly lies in this district pursuant to 28 U.S.C. § 1391. Defendant maintains its principal place of business in this District, Defendant regularly

transacts business in this District, and many of the acts and transactions giving rise to this action occurred in this District.

GENERAL ALLEGATIONS

11. Target is an American discount retailer or "superstore," selling a wide array of consumer merchandise such as clothing, home furnishings, foodstuffs, electronics, books, toys, and pharmaceuticals. It is the second-largest discount retailer in the United States – behind Walmart – with 1,797 locations spread across the country.

12. On December 18, 2013, security researcher and blogger Brian Krebs reported[4] that Target was investigating a massive data breach, in which unknown third parties illegally obtained information related to Target customers' credit and debit cards, including the customers' names, credit/debit card number, the card's expiration date, and the card's CVV.[5]

13. According to Krebs, the data breach began on November 27, 2013 – also known as "Black Friday," typically the busiest shopping day of the year in the United States – and continued until at least December 15, 2013.

[4] Brian Krebs, "Sources: Target Investigating Data Breach," *Krebs on Security* (Dec. 18, 2013) (available at http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/).

[5] "Card Verification Value" – a CVV is an authentication code, embedded on the magnetic stripe of a payment card and used for "card present" transactions (*i.e.*, transactions in which the physical card is used to transmit payment information; in contrast to purchases made online, for example). The purpose of the CVV is to verify that the payment card is actually in the possession of the merchant. The CVV is automatically retrieved when the magnetic stripe of a card is swiped on a point-of-sale (card present) device and is verified by the issuer.

14. Per Krebs' sources, Target became aware of the breach at some point during this period. However, at *no point* prior to Krebs' article did the Company take *any* steps to alert its customers, or their financial institutions, that their critically sensitive financial information was in the hands of thieves.

15. Indeed, only upon the publication of Krebs' article was Target moved to respond. On December 19, 2013, a full day after the original story broke, Target posted a statement on its website – and no other mechanism of publication – acknowledging the breach.

16. At present, news reports have confirmed that 40 million Target customers have had their sensitive financial data – at a minimum, their names, card numbers, card expiration dates, and card CVVs – stolen by criminals.[6]

17. Target has also revealed that as a result of the same data breach, the names, mailing addresses, phone numbers, and email addresses for up to 70 million customers have been compromised.[7]

18. Additionally, subsequent admissions by Target reveal that, for purchases in which customers supplied their PIN[8] at the point of sale thieves also obtained that information.[9]

---

[6] Elizabeth A. Harris, "For Target's Shoppers, a New Holiday To-Do List," *N.Y. Times* (Dec. 19, 2013) (available at http://www.nytimes.com/2013/12/20/business/for-targets-shoppers-a-new-holiday-to-do-list.html?ref=targetcorporation).

[7] Larry Dignan, "Target's Data Breach: It Gets Worse." *ZDNet* (Jan. 10, 2013) (available at http://www.zdnet.com/targets-data-breach-it-gets-worse-7000025024/).

[8] A Personal Identification Number or "PIN" is a four digit, secret code that customers use to authenticate certain debit card purchases and ATM cash withdrawals.

19. Further, it is a certainty that thieves not only *have* these items of information, they are also actively *selling* these data on the black market, for purposes of identity theft and bank fraud. In a follow up to his initial story, Brian Krebs documented a search of a black market credit and debit card data brokerage site, in which cards stolen from the data breach were being bought and sold:

> [M]y source at the big bank had said all of the cards his team purchased from this card shop that matched Target's Nov. 27 – Dec. 15 breach window bore the base name Tortuga, which is Spanish for "tortoise" or "turtle."
>
> Indeed, shortly after the Target breach began, the proprietor of this card shop — a miscreant nicknamed "Rescator" and a key figure on a Russian-language cybercrime forum known as "Lampeduza" — was advertising a brand new base of one million cards, called Tortuga.
>
> Rescator even . . . advertis[ed a] "valid 100% rate," and offer[ed] a money-back guarantee on any cards from this "fresh" base that were found to have been canceled by the card issuer immediately after purchase. In addition, sometime in December, this shop ceased selling cards from other bases aside from those from the Tortuga base. As the month wore on, new Tortuga bases would be added to shop, with each base incrementing by one with almost every passing day (e.g., Tortuga1, Tortuga2, Tortuga3, etc.).
>
> Another fascinating feature of this card shop is that *it appears to include the ZIP code and city of the store from which the cards were stolen*. One fraud expert I spoke with who asked to remain anonymous said this information is included to help fraudsters purchasing the dumps make same-state purchases, thus avoiding any knee-jerk fraud defenses in which a

[9] Sam Sanders, "Target's Word May Not Be Enough To Keep Your Stolen PIN Safe." *NPR* (Dec. 29, 2013) (available at http://www.npr.org/2013/12/29/258009006/targets-word-may-not-be-enough-to-keep-your-stolen-pins-safe).

> financial institution might block transactions out-of-state from a known compromised card.[10]

20. While Target offers a vague assurance that it has "identified and resolved the issue," in the same statement the Company directs readers to anti-fraud websites of the FTC, credit reporting bureaus, and state Attorney Generals' offices.[11]

21. Further, despite the Company's equivocating statements on the issue, it is still unknown how such a systemic, cataclysmic act of theft could be perpetuated. While some reports suggest that the thieves placed small chips into the credit card readers at the Company's checkout lanes – a criminal act commonly referred to as "skimming" – other researchers note the improbability of such a massively coordinated effort (again, Target's stores number almost 1,800 nationwide), and instead suggest either malicious software or even an organized effort from within the Company.[12]

DEFENDANT'S CONDUCT HAS HARMED PLAINTIFF AND CLASS MEMBERS

22. Plaintiff is a commercial bank, maintaining and administering the accounts of customers that include persons and/or entities that made purchases at Target stores during the period of November 27, 2013 to December 15, 2013, using debit cards

[10] Brian Krebs, "Cards Stolen in Target Breach Flood Underground Markets," *Krebs on Security* (Dec. 20, 2013) (available at http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/).

[11] Gregg Steinhafel, "A Message From CEO Gregg Steinhafel About Target's Payment Card Issues," (Dec. 20, 2013) (available at https://corporate.target.com/discover/article/important-notice-unauthorized-access-to-payment-ca).

[12] Antone Gonsalves, "Target Breach Likely Involved Inside Knowledge, Experts Say," *PC World* (Dec. 21, 2013) (available at http://www.pcworld.com/article/2082268/target-breach-likely-involved-inside-knowledge-experts-say.html).

issued by Plaintiff. Accordingly, the sensitive financial data of Plaintiff's customers, including names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs, have been obtained by thieves.

23. Thieves could not have accessed this information – either via "skimming" from Target's point-of-sale machines, installing some type of malicious software in the Company's infrastructure, or utilizing Company insiders to otherwise obtain these data – but for Defendant's negligence.

24. Target failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach described in this Complaint, despite being on notice that its security protocols were especially vulnerable to cyber-attack.

a. Since at least 2007, Target has been or should have been aware of its vulnerability to theft of consumer data.

25. Between 2005 and 2007, a criminal named Albert Gonzalez masterminded one of the largest coordinated data breaches in history, ultimately compromising more than 170 million credit and debit card accounts. Gonzalez executed his attack by infecting retailers' Point of Sale terminals ("POS machines")[13] with malware (malicious software that infects the POS machine) which transmitted, unencrypted, the financial data being processed by the POS machine to Gonzalez and his

[13] A Point of Sale terminal ("POS machine") is the machine that processes a consumer's credit or debit card at the point of sale. Typically, these are the machines at the checkout register that enable customers to swipe their credit or debit cards. The POS machine then processes the information on the consumer's credit or debit card to authorize the sale.

accomplices.[14] While the brunt of the payment card information stolen was obtained from the networks of the payment processor Heartland Payment Systems and the retailer TJ Maxx, following Gonzalez's criminal trial Target admitted that it, too, had been a victim of the cyber-attack.[15] When asked about the integrity of its own security measures, and whether the Company was in some way culpable for the compromise of customers' financial data, Target simply responded that "[a] previously planned security enhancement was already under way at the time the criminal activity against Target occurred."[16]

26. Subsequently, in April of 2011, Target informed its customers that their names and email addresses had been exposed in a data breach suffered by Epsilon, a third-party marketing firm hired by Target.[17] While the number of affected customers is unknown, at the time analysts believed the breach to be one of the largest, ever.[18]

27. Finally, in the months leading up to the data breach at issue in this litigation, Target received multiple warnings from Visa – first in April, 2013 and then in August of the same year – stating that Visa had "seen an increase in network intrusions involving retail merchants," where hackers were able to install malware that would

[14] James Verini, "The Great Cyberheist," *N.Y. Times* (Nov. 10, 2010) (available at http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?pagewanted=all&_r=0).
[15] Jim Finkle, "Target Co. Was Victim of Hacker Albert Gonzalez," *Reuters* (Dec. 30, 2009) (available at http://www.reuters.com/article/2009/12/30/us-hacker-idUSTRE5BS3LU20091230).
[16] *Id.*
[17] Maria Aspan and Martinne Geller, "US Data Breach Hits Target, Marriott Customers," *Reuters* (Apr. 5, 2011) (available at http://www.reuters.com/article/2011/04/05/uk-epsilon-factbox-idUSLNE73401B20110405).
[18] Miguel Helft, "After Breach, Companies Warn of E-Mail Fraud," *N.Y. Times* (Apr. 4, 2011) (available at http://www.nytimes.com/2011/04/05/business/05hack.html).

"extract full magnetic stripe data" from retailers' payment processing machines. Visa issued these alerts "to make clients aware of new malware information . . . *and to remind Visa merchants to secure their payment processing (and non-payment) networks from unauthorized access*."[19] The bulletins went on to provide best security practices for, *inter alia*, "Cash Register and POS Security" and "Network Security."[20]

28. Thus, at the time of the data breach occurring on or about November 27, 2013, and continuing to on or about December 15, 2013, Target had been put on notice by *two previous data breaches and two explicit warnings from Visa*, all indicating that Target's networks and POS machines were at risk of cyber-attack.

b. Target violated industry mandate and state statutes where it failed to provide adequate protections of consumers' financial data.

29. Defendant, as a retailer that accepts payment cards such as debit and credit cards, has entered into agreements with major payment card brands – including Visa and MasterCard – to comply with a security standard known as the Payment Card Industry Security Standard ("PCI DSS"). The PCI DSS requires retailers to abide by twelve overarching standards:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data.

[19] Visa bulletin, "Retail Merchants Targeted by Memory-Parsing Malware UPDATE," (Aug. 2013) (available at http://usa.visa.com/download/merchants/Bulletin_Memory_Parser_Update_082013.pdf); *see also* "Preventing Memory-Parsing Malware Attacks on Grocery Merchants," (Apr. 11, 2013) (available at http://usa.visa.com/download/merchants/alert-prevent-grocer-malware-attacks-04112013.pdf).

[20] *Id.*

2. Do no use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across open, public networks.

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security.[21]

[21] *PCI DSS Requirements and Security Assessment Procedures* (Nov. 2013) (available at https://www.pcisecuritystandards.org/security_standards/documents.php).

30. Following news of the data breach, industry professionals have been quick to note that the specific data compromised prove to a certainty that Target was not PCI DSS compliant. As a respected security professional stated:

> This is a breach that should've never happened. The fact that three-digit CVV security codes were compromised shows they were being stored. *Storing CVV codes has long been banned by the card brands and the PCI [Security Standards Council]*.[22]

31. Additionally, pursuant to the PCI DSS, neither customer PINs nor the Full Magnetic Stripe Data are supposed to be stored by retailers, and thus by the same logic, should not have been able to be compromised by thieves.

Technical Guidelines for PCI Data Storage

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name[1]	Yes	Yes[1]	No
	Service Code[1]	Yes	Yes[1]	No
	Expiration Date[1]	Yes	Yes[1]	No
Sensitive Authentication Data[2]	Full Magnetic Stripe Data[3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

[23]

32. This retention of data forbidden under the PCI DSS, well outside the scope of typical payment card industry protocol, proved to be a boon to the thieves:

---

[22] Matthew J. Schwartz, "Target Breach: 10 Facts," *Information Week* (Dec. 21, 2013) (quoting John Kindervag of Forrester Research) (available at http://www.informationweek.com/security/attacks-and-breaches/target-breach-10-facts/d/d-id/1113228)

[23] John Casaretto, "Target's Big Mess: Customer PIN Information Part of Breach," *SiliconAngle* (Dec. 27, 2013) (available at http://siliconangle.com/blog/2013/12/27/targets-big-mess-customer-pin-information-part-of-breach/).

> [T]he criminals discovered that Target's systems were ***astonishingly open*** — lacking the virtual walls and motion detectors found in secure networks like many banks'. Without those safeguards, the thieves moved swiftly into the company's computer servers containing Target's customer data and to the crown jewel: the in-store systems where consumers swipe their credit and debit cards and enter their PINs.[24]

33. Ultimately, Target's inexcusable failure to comply with industry-standard data protection and retention practices, resulting in a "new world record" for "the sheer volume of data stolen over time" has left security experts confounded by the Company's negligence:

> "This is the worst breach in history," Ken Stasiak, CEO of SecureState, told NBC News. "It's 2014. We expect retailers of this magnitude to have better security, weigh their risks and spend the resources necessary to secure their data."[25]

34. Indeed, to security industry professionals such as Chester Wisniewski, an adviser for the computer security firm Sophos, it is "obvious" that Target's security protocols, including its data retention procedures, establish the Company's culpability in this matter. Per Wisniewski, "If normal practices were followed, [the thieves] wouldn't have been able to get access."[26]

---

[24] *Id*. (emphasis added).

[25] Keith Wagstaff, "'Worst Breach in History' Puts Data Security Pressures on Retail Industry," *NBC News* (Jan. 10, 2014) (available at http://www.nbcnews.com/technology/worst-breach-history-puts-data-security-pressure-retail-industry-2D11898690).

[26] Joe Mandak, "Thieves May Have Used Pa. Company to Hit Target," *Associated Press* (Feb. 7, 2013) (available at http://www.washingtonpost.com/business/pa-vendor-confirms-link-to-target-data-probe/2014/02/07/e4680ada-8ffe-11e3-878e-d76656564a01_story.html).

35. Fueled by the exact sentiment expressed by Wisniewski, and in the wake of data breaches compromising hundreds of millions if not *billions* of consumers' financial data, several states have enacted statutes requiring retailers to strictly comply with the PCI DSS. Where retailers do not adhere to this industry-mandated standard of care, financial institutions may seek actual damages for costs incurred as a result of the retailer's noncompliance. Among the states enacting such statutes is Minnesota, home of Target's corporate headquarters.[27]

36. In addition, Oregon law establishes data security standards for an entity that "owns, maintains or otherwise possesses data" that have been characterized as some of the most exacting in the nation, enumerating myriad administrative, technical, and physical safeguards that companies like Target must fully implement, and which Target failed to fully implement.[28]

37. As a result of Target's noncompliance with standards mandated both by industry and state statutes, the sensitive financial data of Plaintiff's and Class Members' customers – including names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs – are not only in the hands of thieves, but are brazenly being trafficked on black market websites.

---

[27] Minn. Stat. § 325E.64.

[28] Or. Rev. Stat. § 646A.622; *See also* Scott Cooper, Navid Soleymani, Clifford Davidson, & Tanya Forsheit, *State Privacy Laws*, *in* Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age § 5:5:6 (Practicing Law Institute, last updated September 2013) (stating that "in most cases" states imposing data security standards by statute are "less detailed than Oregon's law").

38. Accordingly, and as a result of Defendant's conduct, Plaintiff and Class Members experienced losses in the form of reissuing payment cards and refunding fraudulent charges for customer accounts affected by Target's data breach, as well as costs associated with notifying customers.[29]

39. Plaintiff incurred these costs not simply to preemptively assuage its customers' concerns arising from Target's latest data breach – although this was of paramount importance to Plaintiff – but also because it is Plaintiff, along with Class Members, who must bear the cost of any fraudulent charges made by thieves in possession of these compromised financial data. Put another way: in situations such as these, where *over 100 million consumer accounts have been compromised and are being actively traded on the black market*, financial institutions become the *de facto* insurer of the negligent retailer. While it is, of course, unfair to expect a consumer to bear costs arising from a crime that he or she was in no position to guard against, it is equally unfair to expect a financial institution – who is in no better position to control the security protocols of a given retailer or to even be *aware* of security breaches suffered by a retailer – to incur costs arising from a retailer's negligence. As stated to Congress by Frank Keating, the President and CEO of the American Bankers Association:

> **Banks Protect Consumers:** In breaches like that of Target's, the banking industry's first priority is to protect consumers and make them whole. When a retailer like Target speaks of its customers having "zero liability" from fraudulent transactions, it is because our nation's banks are providing that relief, not the retailer that suffered the breach. It is often

[29]Notification of customers is a major component of most financial institutions' costs in responding to this type of event.

> the case that banks must explain to their customers what has happened without the bank knowing where the breach has occurred. Moreover, bankers have historically received little meaningful reimbursement for the costs they have incurred.[30]

40. Moreover, as Keating's letter goes on to note, this criminal threat continues to grow.[31] At the time of Albert Gonzalez's criminal trial in 2009, the scope of a data breach in which over 100 million payment cards were compromised was *staggering*. Four years later, such numbers threaten to become commonplace.

41. Yet no appreciable changes in the security of retailers' POS machines or networks appear to have occurred. Instead, Target's CEO Gregg Steinhafel has assured consumers that "they will not be held financially responsible for any credit and debit card fraud."[32] Such a statement, while true, is also disingenuous, as it fails to mention that this is so simply because *banks* are required to cover losses arising from such types of fraud.

42. Moreover, left unchecked, these repeated failures on the part of retailers to adhere to industry-mandated standards of care will eventually erode consumer confidence. Indeed, this is one of the immediate effects of the latest Target data breach.[33] Decline in financial institutions' card impact and card loyalty can be devastating to the

---

[30] Frank Keating, American Bankers Association, Letter to members of the U.S. Senate and House of Representatives, "Target Data Breach," (Jan. 16, 2014) (available at http://www.aba.com/Advocacy/LetterstoCongress/Documents/DataSecurity-CongressMemoReTargetBreach-011614.pdf).

[31] *Id*. at 2.

[32] Gregg Steinhafel, "A Message From CEO Gregg Steinhafel About Target's Payment Card Issues," (Dec. 20, 2013) (available at http://pressroom.target.com/news/a-message-from-ceo-gregg-steinhafel-about-targets-payment-card-issues).

[33] Arte Levy, "Restoring the Faith: Rebuilding Consumer Confidence in the Wake of a Data Breach," *Yahoo! Small Business Advisor* (Feb. 19, 2014) (available at http://smallbusiness.yahoo.com/advisor/restoring-faith-rebuilding-consumer-confidence-wake-data-breach-175515514.html).

institutions' revenue, and such variables are fueled by the customer's belief that the card at issue is a secure payment mechanism.

43. Beyond the immediate and the intangible injuries suffered by Plaintiff and Class Members, Defendant's conduct creates additional, future risk of bank fraud and other, criminal harm. The myriad risks posed to victims of data breaches – including financial institutions – unveil themselves over periods of years, not days or even months. As the Government Accountability Office has noted in a report on data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

44. Ultimately, then, Plaintiff and Class Members have suffered – and will continue to face – a panoply of threats, from the immediate and concrete, to the very long-term.

CLASS ALLEGATIONS

45. Plaintiff brings this action, pursuant to Rule 23 of the Federal Rules of Civil Procedures, individually and on behalf of all Members of the following classes (collectively referred to as "the Class" or "Class"):

[34] Government Accountability Office, "Report to Congressional Requesters," at 33 (Jun. 2007) (available at http://www.gao.gov/new.items/d07737.pdf).

> **National Class:** All financial institutions – including banks and credit unions – in the United States that have had the confidential financial data associated with their customers' accounts – including but not limited to customer names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs – compromised as a result of the data breach at Target stores from the period beginning on or about November 27, 2013, and ending on or about December 15, 2013.
>
> **Oregon Sub-Class:** All financial institutions – including banks and credit unions – in the State of Oregon that have had the confidential financial data associated with their customers' accounts – including but not limited to customer names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs – compromised as a result of the data breach at Target stores from the period beginning on or about November 27, 2013, and ending on or about December 15, 2013.

46. Excluded from the Class are the following individuals and/or entities: Target and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Target has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family Members.

47. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

48. The Class is so numerous that joinder of all Members is impracticable. The number of separate individuals whose private financial data have been compromised

as a result of the data breach described herein number at approximately 110 million, making the number of affected financial institutions – all of whom are members of the proposed Class – number in at least the thousands.

49. There are questions of law or fact common to the Class. These questions include, but are not limited to, the following:

a. Whether Defendant's retention of financial data post-transaction violated Minn. Stat. § 325E.64;

b. Whether Defendant was negligent in the development, use, or maintenance of its security protocols, failing to exercise a reasonable standard of care due in the circumstances;

c. Whether Defendant's violations of Minn. Stat. § 325E.64 amounted to negligence *per se*;

d. Whether Defendant's actions were unlawful under Minn. Stat. § 325F.69;

e. Whether Defendant's actions were deceptive under Minn. Stat. § 325D.44;

f. Whether Defendant acted willfully and/or with oppression, fraud, or malice;

g. Whether Defendant's conduct constituted Bailment;

h. Whether Defendant's conduct constituted Conversion;

i. Whether Defendant's actions breached duties imposed under Or. Rev. Stat. § 646A.600, *et seq.*;

j. Whether Defendant's actions violated Or. Rev. Stat. § 646.605, *et seq.*; and

k. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

50. Plaintiff's claims are typical of the claims of the Class in that Plaintiff and Class Members experienced losses, as a result of Defendant's conduct, in the form of reissuing debit cards and refunding fraudulent charges for accounts affected by Target's data breach, as well as incurring costs for the notification of its customers.

51. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff's interests do not conflict with the interests of the Class Members. Furthermore, Plaintiff has retained competent counsel experienced in class action litigation. Plaintiff's counsel will fairly and adequately protect and represent the interests of the Class.

52. Plaintiff asserts that pursuant to Fed. R. Civ. P. 23(b)(3), questions of law or fact common to the Class Members predominate over any questions affecting only individual Members.

53. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Even if Class Members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, and considering that the parties affected by Target's data breach number in the tens of millions or greater, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a

class action presents far fewer management difficulties, allows claims to be heard which may otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT ONE
(Violation of Minn. Stat. § 325E.64)
(Brought on behalf of the Class)

54. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

55. The Minnesota Legislature, in an effort to combat cybercrime and to protect financial institutions from negligent practices of retailers, enacted Minn. Stat. § 325E.64, which states in pertinent part:

> 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.

56. Plaintiff and Class Members are "financial institutions" within the meaning of Minn. Stat. § 325E.64.

57. As alleged in this Complaint, Defendant violated the above-quoted provisions of Minn. Stat. § 325E.64, at minimum, when it retained Plaintiffs' and Class

Members' customers' card security code data, PIN verification code numbers, and/or the full contents of any track of magnetic stripe data, subsequent to the authorization of the customers' transactions. Further, in the case of a PIN debit transaction, Target violated Minn. Stat. § 325E.64 when it held such data subsequent to 48 hours after authorization of the customers' transactions.

58. Accordingly, pursuant to Minn. Stat. § 325E.64, Plaintiff and Class Members are entitled to reimbursement from Defendant 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."

COUNT TWO
(Violation of Minn. Stat. § 325F.69)
(Brought on behalf of the Class)

59. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

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

61. Defendant's conduct as alleged herein constitutes an unlawful business practice as proscribed by Minn. Stat. § 325F.69.

62. Defendant represented to its customers – and Plaintiff's account holders – that it would abide by the PCI DSS, where it: (1) displayed the insignias of Payment Card Industry members (including Visa and MasterCard); and (2) processed payments via payment cards of Payment Card Industry members. Both such actions created an impression that Defendant was PCI DSS compliant as, in order to accept payments using

those Payment Card Industry affiliates, Defendant would have agreed to comply with the PCI DSS.

63. However, as alleged in this complaint, Defendant did *not* comply with the PCI DSS as, *inter alia*, Defendant stored sensitive authentication data including cardholder's PINs and CVVs, and retained sensitive financial data for impermissibly long periods of time. Such acts are prohibited by the PCI DSS.

64. Such misrepresentations, made to the public at large, caused substantial damage to Plaintiff and Class Members, and had a direct and substantial effect in Minnesota and throughout the United States.

65. The misrepresentations described above – amounting to unlawful business practices – were relied upon by Plaintiff and Class Members, who suffered damages as a result.

COUNT THREE
(Violation of Minn. Stat. § 325D.43, *et seq.*)
(Brought on behalf of the Class)

66. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

67. Defendant's conduct as alleged herein constitutes a deceptive business practice as proscribed by the Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.43, *et seq.*

68. Pursuant to Minn. Stat. § 325D.44, a corporation violates the Minnesota Uniform Deceptive Trade Practices Act when it "represents that . . . services have . . . characteristics . . . that they do not have," or "engages in any other conduct which

similarly creates a likelihood of confusion or of misunderstanding." Minn. Stat. § 325D.44, subd. 1(5) & (13). Here, Defendant implied association with and certification by the Payment Card Industry, which two items are predicated on PCI DSS compliance. Similarly, Defendant violated this blanket prohibition on deceptive acts and practices by implying that it would adhere to a standard of care articulated by the Payment Card Industry – a well-established prerequisite to processing payment card transactions – which Defendant did not do.

69. Defendant represented to its customers – and Plaintiff's account holders – that it would abide by the PCI DSS, where it (1) displayed the insignias of Payment Card Industry members (including Visa and MasterCard) and (2) processed payments via payment cards of Payment Card Industry members. Both such actions created an impression that Defendant was PCI DSS compliant as, in order to accept payments using those Payment Card Industry affiliates, Defendant would have agreed to comply with the PCI DSS.

70. However, as alleged in this complaint, Defendant did *not* comply with the PCI DSS as, *inter alia*, Defendant stored sensitive authentication data including cardholder's PINs and CVVs, and retained sensitive financial data for impermissibly long periods of time. Such acts are prohibited by the PCI DSS.

71. Finally, the Uniform Deceptive Practices Act is to be "very broadly construed," due to its remedial purpose, and general acts of fraud committed in the course of business are, as a practical matter, proscribed by the statute. *State by Humphrey v. Philip Morris, Inc.*, 551 N.W.2d 490, 496 (Minn. 1996). When Defendant represented to

its customers that it would adhere to certain, minimal security standards, and when Defendant did not, in fact, adhere to those security standards, Defendant violated the Uniform Deceptive Practices Act.

72. Plaintiff and Class Members seek an order to enjoin Defendant from such deceptive practices, to restore to Plaintiff and Class Members their interest in money or property that may have been acquired by Defendant by means of its deceptive practices, and costs and attorneys' fees.

COUNT FOUR
(Negligence)
(Brought on behalf of the Class)

73. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

74. Defendant owed Plaintiff and Class Members a duty to exercise reasonable care in the acquisition, maintenance, and storage of their customers' financial information, including names, card numbers, card expiration dates, card CVVs, and customer PINs. Such duty includes the implementation of security infrastructure and protocols, including adherence to the PCI DSS.

75. Defendant also owed Plaintiff and Class Members a duty to timely disclose the nature and extent of the data breach extending from November 27, 2013, to December 15, 2013.

76. As alleged herein, Defendant breached its duty to Plaintiff and Class Members where it failed to exercise reasonable care by maintaining adequate security

infrastructure and protocols, thereby failing to safeguard Plaintiff's and Class Members' customers' financial information.

77. As alleged herein, Defendant breached its duty to Plaintiff and Class Members where it failed to timely alert affected consumers to the existence – as well as the depth and breadth – of the data breach extending from November 27, 2013, to December 15, 2013.

78. Defendant's breach of duty proximately caused injury to Plaintiff and Class Members, including losses in the form of reissuing debit cards and refunding fraudulent charges for accounts affected by Target's data breach, as well as incurring costs for the notification of its customers.

79. Plaintiff seeks an award of actual damages individually and on behalf of the Class.

COUNT FIVE
(Bailment)
(Brought on behalf of the Class)

80. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

81. Through their customers, Plaintiff and all other Class Members delivered and entrusted their customers' financial information to Defendant for the sole purpose of allowing private, secure, and one-time financial transactions with Defendant.

82. A bailment arises where possession, but not ownership, of property is transferred from one party ("bailor") to another ("bailee"). Where a bailee has received a

bailment from a bailor, a duty of care is owed. Typically, a bailee is strictly liable for the bailment.

83. During the period of bailment Defendant, as bailee, owed Plaintiff and all other Class Members a duty of care to safeguard their customers' financial information – including names, card numbers, card expiration dates, card CVVs, and customer PINs – by maintaining reasonable security procedures and practices to protect such information. As alleged herein, Defendants breached this duty.

84. As a result of Defendants' breach of this duty, Plaintiffs and all other Class Members have been harmed as alleged herein.

COUNT SIX
(Conversion)
(Brought on behalf of the Class)

85. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

86. Plaintiff and Class Members legally recognized ownership interest in the financial data of their customers that was unlawfully obtained in Target's data breach, including but not limited to the compromised card numbers, card expiration dates, card CVVs, and PINs.

87. Defendant intentionally took, interfered with, or exercised dominion or control over these above-described financial data improperly.

88. Target had and continues to have a duty to maintain and preserve – and most importantly, *secure* – any and all financial data in its possession, in order to prevent its compromise through its own wrongful acts.

89. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered injury and therefore seek compensatory damages.

90. Defendant's conduct was wanton, engaged in with malice and oppression, and in conscious disregard of Plaintiff's and Class Members' rights to their customers' unblemished financial data. As a result of the egregious nature of Defendant's behavior, Plaintiff seeks punitive damages individually and on behalf of the Class.

COUNT SEVEN
(Negligence *Per Se*)
(Brought on behalf of the Class)

91. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

92. Pursuant to Minn. Stat. § 325E.64 Defendant had a duty to comply with the standards set forth in the PCI DSS.

93. Defendant's improper retention of CVV and PIN data, and retention of all data used in consumer financial transactions for a period greater than 48 hours after the authorization of the transaction, amounted to a violation of Minn. Stat. § 325E.64.

94. Such violation of Minn. Stat. § 325E.64 – a statutorily imposed duty of care – amounts to conclusive evidence of duty and breach.

95. Defendant's violation of Minn. Stat. § 325E.64 was the proximate cause of Plaintiff's damages, as alleged herein.

96. But for Defendant's negligent and wrongful breach of its duties owed to Plaintiff and the Class, Plaintiff and the Class would not have been harmed, as alleged herein.

97. Plaintiff and Class Members are members of the class of persons intended to be protected by Minn. Stat. § 325E.64, and the injuries sustained by Plaintiff and Class Members are the type intended to be prevented by Minn. Stat. § 325E.64.

98. Plaintiff and the Class suffered actual damages including, but not limited to: losses in the form of reissuing debit cards and refunding fraudulent charges for accounts affected by Target's data breach, as well as incurring costs for the notification of its customers.

COUNT EIGHT
(Negligent Misrepresentation)
(Brought on behalf of the Class)

99. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

100. Through its processing of payment cards in a variety of payment card systems, including Visa and MasterCard, and through its representations that it processes payments in same and therefore is inherently bound to comply with the PCI DSS, Defendant made false representations and nondisclosures.

101. As discussed in paragraphs 19-21, *supra*, at a minimum, Defendant failed to comply with PCI DSS where it stored customers' CVV codes and PINs.

102. Moreover, Defendant failed to comply with PCI DSS where it improperly retained confidential data and failed to properly protect and safeguard confidential customer data.

103. Defendant's representations that it participated as a member of the payment card systems within the PCI – and therefore implicitly should be compliant with the PCI DSS – were material facts upon which Plaintiff justifiably relied by issuing debit cards to its customers, agreeing to process transactions related to purchases from Target, and acting as issuing financial institutions for transactions related to Target. Plaintiff issued debit cards and processed transactions involving same based upon the expectation that Target would comply with the PCI DSS, thereby safeguarding the financial data that was in fact compromised in the data breach described herein.

104. Defendant did not comply with the PCI DSS, and thus failed to safeguard the confidential financial information that was compromised as a result of the data breach described herein.

105. Defendant knew or should have known that it was not in compliance with the PCI DSS, and that it was generally not adequately safeguarding the confidential information compromised as a result of the data breach complained of herein.

106. Defendant failed to exercise reasonable care in making these representations and/or failing to disclose these items of information upon which Plaintiff reasonably relied.

107. But for Defendant's misrepresentations and non-disclosures, Plaintiff would have undertaken additional efforts to prevent the compromise of its customers' private personal and financial data.

108. As a direct and proximate result of Defendant's misrepresentations and/or non-disclosures, Plaintiff has suffered damages, in an amount to be determined at trial, including but not limited to losses in the form of reissuing debit cards and refunding fraudulent charges for accounts affected by Target's data breach, as well as incurring costs for the notification of its customers.

COUNT NINE
(Breach of Implied Contract)
(Brought on behalf of the Class)

109. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

110. An implied contract existed between Defendant and Plaintiff and Class Members, evidenced, *inter alia*, by Defendant's representations that as a merchant processing payment cards in the PCI member systems, it would comply with the requirements of the PCI DSS and would exercise due care in the safeguarding of the financial data implicated in payment card transactions, and by Plaintiff and Class Members issuing debit cards to their customers, agreeing to process transactions related to purchases from Target, and acting as issuing financial institutions for transactions related to Target. Plaintiff and Class Members issued debit cards and processed transactions involving same based upon the expectation that Target would comply with

the PCI DSS, thereby safeguarding the financial data that was in fact compromised in the data breach described herein.

111. Plaintiff and Class Members would not have entrusted their customers' sensitive financial information to Defendant in the absence of such an implied contract.

112. Defendant breached its implied contract with Plaintiff and Class Members where it failed to comply with the PCI DSS and failed to safeguard the financial information compromised in the data breach described herein.

113. As a result of Defendant's breach, Plaintiff and Class Members suffered damages, including but not limited to losses in the form of reissuing debit cards and refunding fraudulent charges for accounts affected by Target's data breach, as well as incurring costs for the notification of its customers.

114. It would be unfair – and Defendant would be unjustly enriched – were Defendant allowed to retain the benefits it obtained as a result of its implied contract with Plaintiff and Class Members, in light of Defendant's breach.

COUNT TEN
(Negligence *Per Se*)
(Brought on behalf of the Oregon Sub-Class)

115. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

116. Pursuant to the Oregon Consumer Identity Theft Protection Act, Or. Rev. Stat. § 646A.600, *et seq.* ("OCITPA"), Defendant had a duty to comply with the stringent data security standards set forth in the OCITPA.

117. Defendant is a "person" within the meaning of Or. Rev. Stat. § 646A.602(10).

118. In the ordinary course of its business, Defendant owned, maintained, or otherwise possessed "personal information," within the meaning of Or. Rev. Stat. § 646A.602(11).

119. Pursuant to Or. Rev. Stat. § 646A.622(d), Defendant was required to "implement[] an information security program that includes the following:"

> **(A) Administrative safeguards such as the following, in which the person:**
>
> > (i) Designates one or more employees to coordinate the security program;
> >
> > (ii) Identifies reasonably foreseeable internal and external risks;
> >
> > (iii) Assesses the sufficiency of safeguards in place to control the identified risks;
> >
> > (iv) Trains and manages employees in the security program practices and procedures;
> >
> > (v) Selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
> >
> > (vi) Adjusts the security program in light of business changes or new circumstances;
>
> **(B) Technical safeguards such as the following, in which the person:**
>
> > (i) Assesses risks in network and software design;
> >
> > (ii) Assesses risks in information processing, transmission and storage;

> (iii) Detects, prevents and responds to attacks or system failures; and
>
> (iv) Regularly tests and monitors the effectiveness of key controls, systems and procedures; and
>
> **(C) Physical safeguards such as the following, in which the person:**
>
> (i) Assesses risks of information storage and disposal;
>
> (ii) Detects, prevents and responds to intrusions;
>
> (iii) Protects against unauthorized access to or use of personal information during or after the collection, transportation and destruction or disposal of the information; and
>
> (iv) Disposes of personal information after it is no longer needed for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed.

120. Defendant's myriad acts and omissions including, *inter alia*, improper retention of CVV and PIN data, and retention of all data used in consumer financial transactions for a period greater than 48 hours after the authorization of the transaction, failing to heed the April 2013 and August 2013 warnings of Visa, and failing to implement the "virtual walls and motion detectors found in secure networks" (thus leaving its security systems "astonishingly" open) amount to violations of Or. Rev. Stat. § 646A.622(d).

121. Such violations of Or. Rev. Stat. § 646A.622(d) – a statutorily imposed duty of care – amount to conclusive evidence of duty and breach.

122. Defendant's violations of Or. Rev. Stat. § 646A.622(d) were the proximate cause of Plaintiff's damages, as alleged herein.

123. But for Defendant's negligent and wrongful breach of its duties owed to Plaintiff and the Class, Plaintiff and the Class would not have been harmed, as alleged herein.

124. Plaintiff and Class Members are members of the class of persons intended to be protected by Or. Rev. Stat. § 646A.622(d), and the injuries sustained by Plaintiff and Class Members are the type intended to be prevented by Or. Rev. Stat. § 646A.622(d).

125. Plaintiff and the Class suffered actual damages including, but not limited to: losses in the form of reissuing debit cards and refunding fraudulent charges for accounts affected by Target's data breach, as well as incurring costs for the notification of its customers.

COUNT ELEVEN
(Violation of Or. Rev. Stat. § 646.605, *et seq.*)
(Brought on behalf of the Oregon Sub-Class)

126. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

127. Target's policies and practices relating to its sub-standard security measures for the use and retention of its customers' financial information are violations of Oregon's Unlawful Trade Practices Act ("UTPA"), Or. Rev. Stat. § 646.605, *et seq.*

128. Specifically, Target violated, and continues to violate, the UTPA by failing to take proper precautionary measures with its payment card processing machines and the

financial data of its customers, evidenced *inter alia* by its failure to comply with the PCI DSS and its failure to establish security protocols compliant with Or. Rev. Stat.§ 646A.622(d).

129. Similarly, Target violated, and continues to violate, the UTPA by failing to put a fulsome notification policy in place, where customers' financial information is compromised as a result of a data breach.

130. As a result of Target's violations of the UTPA prohibiting unfair and deceptive acts and practices, Plaintiff and members of the Classes have suffered monetary damages for which the Defendant is liable.

131. Plaintiff and the Class seek actual damages plus interest on damages at the legal rate, as well as statutory and punitive damages, equitable relief, and all other just and proper relief afforded by the UTPA.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38, Plaintiff, individually and on behalf of the Class it seeks to represent, demands a jury on any issue so triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of itself and all Class Members, requests judgment be entered against Defendant and that the Court grant the following:

1. An order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiff is a proper class representative, that Plaintiff's attorneys be appointed Class counsel pursuant to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

2. Judgment against Defendant for Plaintiff's and Class Members' asserted causes of action;

3. Appropriate declaratory relief against Defendant;

4. Preliminary and permanent injunctive relief against Defendant;

5. Equitable relief in the form of restitution and disgorgement of revenues wrongfully obtained as a result of Defendant's wrongful conduct;

6. An award of actual damages and compensatory damages in an amount to be determined;

7. An award of punitive damages;

8. An award of reasonable attorney's fees and other litigation costs reasonably incurred; and

9. Any and all relief to which Plaintiff and the Class may be entitled.

DATED: March 10, 2014

LOCKRIDGE GRINDAL NAUEN P.L.L.P.

By: s/ Gregg M. Fishbein
Richard A. Lockridge (#64117)
Gregg M. Fishbein (#202009)
Robert K. Shelquist (#21310X)
Kate M. Baxter-Kauf (#0392037)

100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
gmfishbein@locklaw.com
ralockridge@locklaw.com
rkshelquist@locklaw.com
kmbaxter-kauf@locklaw.com

Hank Bates
Allen Carney
David Slade
CARNEY BATES & PULLIAM, PLLC
11311 Arcade Drive
Little Rock, AR 72212
Telephone: 501.312.8500
Facsimile: 501.312.8505
hbates@cbplaw.com
acarney@cbplaw.com
dslade@cbplaw.com

Jeffrey D. Boyd
Deborah M. Nelson
NELSON BOYD, PLLC
411 University Street, Suite 1200
Seattle, WA 98101
Telephone: 206.971.7601
boyd@nelsonboydlaw.com
nelson@nelsonboydlaw.com

Attorneys for Plaintiff Umpqua Bank