UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

EMPLOYEES CREDIT UNION, KC POLICE CREDIT UNION, and AMERICAN BANK OF COMMERCE, individually and on behalf of all other similarly situated payment card issuers,	§	**CIVIL ACTION NO. _____**
PLAINTIFFS	§	**CLASS ACTION COMPLAINT AND JURY DEMAND**
v.	§	
TARGET CORPORATION,	§	
DEFENDANT	§	

CLASS ACTION COMPLAINT AND JURY DEMAND

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

Mitchell A. Toups
WELLER, GREEN TOUPS & TERRELL, LLP
2615 Calder Ave., Suite 400
Beaumont, TX 77702
Telephone: (409) 838-0101
Facsimile: (409) 838-6780 (FAX)
Email: matoups@wgttlaw.com

G. Robert Blakey
Professor of Law Emeritus
Notre Dame Law School*
7002 East San Miguel Ave.
Paradise Valley, AZ 85253
Telephone: (574) 514-8220
Email: blakey.1@nd.edu
* Noted for identification only

ATTORNEYS FOR PLAINTIFFS AND THE PUTATIVE CLASS

TABLE OF CONTENTS

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiffs Employees Credit Union, KC Police Credit Union, and American Bank of Commerce (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated payment card issuers nationwide (the "Class Members"), complain of the actions of Defendant Target Corporation ("Target"), and respectfully state the following:

NATURE OF THE CASE

1. This is a RICO case. Target is the second largest general merchandise retailer in the United States. Plaintiffs and Class Members are financial institutions and other entities that issued over 40 million Visa and MasterCard branded credit cards and debit cards (collectively, "payment cards") (including REDcards, Target's proprietary payment cards) that were compromised by an ongoing and continuous data breach within Target's point-of-sale (cash register) system and internal network of systems, from November 27, 2013 through December 15, 2013 (and possibly longer) (the "Target Data Breach" or "Data Breach" or "Breach"). As a direct and/or proximate result of the Breach, Plaintiffs and Class Members have incurred (and will continue to incur) damages to their businesses and/or property in the form of, *inter alia*, expenses to cancel and reissue compromised payment cards, absorption of fraudulent charges made on the compromised payment cards, business destruction, lost profits and/or lost business opportunities.

2. As part of the Target Data Breach, hackers hijacked sensitive information residing on the magnetic stripe of the compromised payment cards. The hackers had an open door into Target's point-of-sale (or cash register) system within its internal network of systems through a refrigeration contractor,[1] an outside Target vendor that Target allowed to link remotely to Target's internal network of systems for purposes of electronic billing, contract submission and

[1] The vendor is Fazio Mechanical Services, Inc. in Pittsburgh, Pennsylvania.

project management. The hackers waltzed through the open door and installed malware on Target's point-of-sale terminals, the red payment card swiping machines at Target checkout counters, in each of Target's approximately 1800 retail locations in the United States. The malware "skimmed" or "scraped" customer names, payment card numbers, expiration dates, CVV codes (Card Verification Value codes), and PIN numbers—also known as "track data"—from payment card transactions, stored the stolen payment card information in a hijacked control server within Target's internal network, and later transmitted the stolen information to the hackers via the Internet.

3. Illicit websites immediately began selling the stolen payment card information "dumps" to international card counterfeiters and fraudsters and issuing financial institutions attempting to mitigate their risk. Crooks can create counterfeit credit cards by encoding the stolen payment card information onto any card with a magnetic stripe, and use the counterfeit cards to make fraudulent purchases. Fraudsters also can create fake debit cards with the stolen payment card information, and withdraw cash from the bank accounts of unsuspecting victims through ATMs. Confirmed fraud involving the stolen payment card information was detected by multiple payment card processing companies well before December 19, 2013, the date Target first reported the Target Data Breach to the general public.

4. Subsequent forensics revealed an additional 70 million identities were stolen and compromised during the Target Data Breach, including personally identifying information ("PII") such as names, mailing addresses, telephone numbers and email addresses. Target disclosed the second component of the Target Data Breach on January 10, 2014, making the Black Friday Target Data Breach one of the most extensive data breaches in history. From a damage perspective, the Target Data Breach is shaping up to be the worst in history as the fraudulent use of the stolen payment card information is pervasive and disturbingly audacious.

5. The Target Data Breach could have been prevented. As early as 2007, Target was warned by a data security expert about the possibility of a data breach in its point-of-sale system. Target was told how to prevent such a breach and, if the preventative measures were not taken, warned that a data breach could result in as many as 58 million payment cards being compromised—an amazingly accurate prophecy. Even though Target described the security expert's suggestions as "good ideas," on information and belief, it did not implement them. On further information and belief, Target also was not in full compliance with the Payment Card Industry Data Security Standards ("PCI DSS").[2]

6. At all relevant times, Plaintiffs and Class Members were (and continue to be) members of the Visa and MasterCard Networks. Since at least 2007 (and possibly earlier), Target engaged in unlawful and intentional schemes to (i) defraud and cheat Plaintiffs and Class Members to obtain money, funds, credits, assets, and/or other property owned by, or under the custody or control of, Plaintiffs and Class Members by means of false or fraudulent pretenses and/or (ii) fraudulently and intentionally misrepresent to Plaintiffs and Class Members—explicitly and/or implicitly—through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate and/or foreign wires, its website, and its participation in the Visa Network and MasterCard Network that (a) it was in compliance with the Visa Operating Regulations and/or MasterCard Rules mandating the protection of payment card information and prohibiting the retention or storage of payment card account numbers, PIN numbers, personal information, magnetic stripe information, and/or transaction information subsequent to the approval of the transaction, (b) it was in compliance with the PCI DSS, and (c) its customer data security policies, procedures, protocols, and

[2] *See* www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0.

hardware and software systems were in place and would safeguard and protect sensitive customer data—including the stolen and compromised payment card information—for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Target and/or approve millions of payment card purchases made at Target via the interstate and/or foreign wires for the further purpose of increasing Target's revenue, profitability, and return on investment. Alternatively, Target fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse was true. By doing so, Target (i) directly and/or proximately caused Plaintiffs and Class Members to suffer damages to their businesses and/or property, (ii) saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (iii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members. Target intentionally engaged in these wrongful actions, inaction and/or omissions for its financial benefit and Plaintiffs' and Class Members' financial detriment.

7. Plaintiffs, for themselves and Class Members, bring this action against Target as a national class action under Title XI ("RICO") of Public Law 91-452, 84 Stat. 922 (1970) (as codified at 18 U.S.C. §§ 1961–1968, as amended) for engaging in the above-described unlawful and intentional schemes. At all relevant times, by its wrongful actions, inaction and/or omissions, Target conducted and participated, directly and/or indirectly, in the affairs of the Visa Network and MasterCard Network (the RICO enterprises) through a pattern of unlawful activity—to wit, Target engaged in repetitious and systematic interstate and/or foreign wire fraud in violation of 18 U.S.C. § 1343 by using or causing the use of the wires in interstate and foreign commerce to intentionally, repeatedly and systematically devise, engage in, condone and/or ratify the above-described schemes to (i) defraud and cheat Plaintiffs and Class Members to obtain money, funds, credits, assets, and/or other property owned by, or under the custody or

control of, Plaintiffs and Class Members by means of false or fraudulent pretenses and/or (ii) fraudulently and intentionally misrepresent to Plaintiffs and Class Members—explicitly and/or implicitly—through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate and/or foreign wires that (a) it was in compliance with the Visa Operating Regulations and/or MasterCard Rules mandating the protection of payment card information and prohibiting the retention or storage of payment card account numbers, PIN numbers, personal information, magnetic stripe information, and/or transaction information subsequent to the approval of the transaction, (b) it was in compliance with the PCI DSS, and (c) its customer data security policies, procedures, protocols, and hardware and software systems were in place and would safeguard and protect sensitive customer data—including the stolen and compromised payment card information. Target's wrongful actions, inaction and/or omissions, as it well knew and intended, and without legal justification, unlawfully cheated Plaintiffs and Class Members out of money, funds, credits, assets, and/ or other property owned by, or under the custody or control of, Plaintiffs and Class Members and/or induced Plaintiffs and Class Members to issue payment cards used to make purchases at Target and/or approve millions of payment card purchases made at Target via the interstate and/or foreign wires with full knowledge its customer data security policies, procedures, protocols, and hardware and software systems, in fact, did not safeguard and protect sensitive customer data—including the stolen payment card information.

8. At all relevant times, by its wrongful actions, inaction and/or omissions, Target (i) conducted or participated in the affairs of the Visa and MasterCard Networks (the RICO enterprises) (in violation of 18 U.S.C. § 1962(c)); and/or (ii) conspired to violate 18 U.S.C. § 1962(a) and (c) (in violation of 18 U.S.C. § 1962(d)).

9. Target agreed to commit (and committed) these substantive RICO offenses (*i.e.*,

the above-described unlawful and intentional schemes through the RICO enterprises (*i.e.*, the Visa Network and MasterCard Network)) by engaging in multiple predicate acts of interstate and/or foreign wire fraud—all the while knowing of, and intentionally agreeing to, the overall objective of the schemes with full knowledge that its customer data security policies, procedures, protocols, and hardware and software systems, in fact, did not safeguard and protect sensitive customer data, including the stolen payment card information—thereby subjecting Plaintiffs and Class Members to, *inter alia*, the risk, expense and obligation of cancelling and reissuing the payment cards and absorbing fraudulent charges made on the compromised payment cards. Target engaged in these schemes for the purpose of increasing its revenue, profitability, and return on investment—to the financial detriment of Plaintiffs and Class Members.

10. Target knew, and intentionally so acted, that Plaintiffs and Class Members are part of the Visa and MasterCard Networks and rely on merchants that accept Visa and MasterCard payment cards to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems—especially in the merchants' point-of-sale systems. Target also knew, and intentionally so acted, that its above-described wrongful actions, inaction and/or omissions were fraudulent, misleading and unlawful, and would unlawfully cheat and defraud Plaintiffs and Class Members in their businesses and/or property, and take unlawful and unfair advantage of Plaintiff and Class Members.

11. In addition to violating the RICO statute, Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions constitute negligent misrepresentation, negligence/gross negligence, negligence *per se*, breach of contract, unfair and deceptive acts and practices in violation of Minn. Stat. § 325F.69, subd. 1, violation of Minn. Stat. § 325E.64, unjust enrichment and/or assumpsit.

12. Plaintiffs, for themselves and Class Members, seek to recover from Target their

(i) actual, consequential, incidental and/or statutory damages, (ii) punitive damages, (iii) RICO treble damages, (iv) equitable relief in the form of disgorgement of gross revenues earned on payment card purchases, (v) injunctive relief to require Target to implement the proper customer data protection policies, procedures, protocols, hardware and/or software systems and discontinue its above-described schemes, wrongful actions, inaction and/or omissions, (vi) pre- and post-judgment interest, (vii) attorneys' fees, litigation expenses, court costs, and (viii) such other relief as the Court may deem just and proper.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over Plaintiffs' claims under (i) 18 U.S.C. § 1961, *et seq.*, under 18 U.S.C. § 1964(a); (c) (RICO); (ii) 28 U.S.C. § 1332(d) (CAFA), because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state diverse from the citizenship of Target, and (c) the matter in controversy exceeds $5,000,000 USD, exclusive of interest and costs; and (iii) 28 U.S.C. § 1367 (supplemental jurisdiction). This Court has *in personam* jurisdiction over Target because at all relevant times, Target resided, was found, had agents, and/or conducted business in the Northern District of Texas.

14. At all relevant times, Target resided, was found, had agents, and/or conducted business in the Northern District of Texas. Accordingly, venue is proper in the Northern District of Texas under 28 U.S.C § 1391(a) and 18 U.S.C § 1965.

PARTIES

15. Plaintiff Employees Credit Union is a Texas financial institution with its principal place of business in Dallas, Texas. ECU issued Visa and MasterCard branded payment cards that were compromised by the Target Data Beach. As a direct and/or proximate result of Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions, ECU has incurred (and/or will continue to incur) damages to its business and/or property in the form

of, *inter alia*, the expenses to cancel and reissue the compromised payment cards it issued and the absorption of fraudulent charges made on the compromised payment cards it issued.

16. Plaintiff KC Police Credit Union ("KCPCU") is a Kansas financial institution with its principal place of business in Kansas City, Kansas. KCPCU issued Visa branded payment cards that were compromised by the Target Data Beach. As a direct and/or proximate result of Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions, KCPCU has incurred (and/or will continue to incur) damages to its business and/or property in the form of, *inter alia*, expenses to cancel and reissue the compromised payment cards it issued and the absorption of fraudulent charges made on the compromised payment cards it issued.

17. Plaintiff American Bank of Commerce ("ABC") is a Texas financial institution with its principal place of business in Wolfforth, Texas. ABC issued MasterCard branded payment cards that were compromised by the Target Data Beach. As a direct and/or proximate result of Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions, ABC has incurred (and/or will continue to incur) damages to its business and/or property in the form of, *inter alia*, expenses to cancel and reissue the compromised payment cards it issued and the absorption of fraudulent charges made on the compromised payment cards it issued.

18. Defendant Target Corporation ("Target") is a Minnesota corporation with its principal place of business in Minneapolis, Minnesota. Target is the second largest general merchandise retailer in America with over 360,000 employees and approximately 1800 stores located throughout the United States. Target's fiscal year 2013 gross revenue was over $73 billion. Target is ranked 36th on the Fortune 500 (2013 list) and is a component of the Standard & Poor's 500 index. Target is publicly traded on the New York Stock Exchange (symbol: TGT). At all relevant times, Target engaged in the above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions that directly and/or proximately caused Plaintiffs and Class

Members to suffer damages to their business and/or property in the form of, *inter alia*, expenses to cancel and reissue the compromised payment cards and the absorption of fraudulent charges made on the compromised payment cards they issued. Target engaged in the above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Target and/or approve payment card purchases made at Target via the interstate and/or foreign wires for the further purpose of increasing Target's revenue, profitability, and return on investment. Target may be served with Summons and a copy of this Class Action Complaint and Jury Demand by serving its registered agent for service of process, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201-3136.

FACTS

I. Payment card transactions on the Visa and MasterCard Networks.

19. The Visa Network and MasterCard Network are principally composed of acquiring banks (*i.e.*, financial institutions that contract with merchants to process their Visa and MasterCard payment card transactions) and payment card issuers (such as Plaintiffs and Class Members).

20. A typical payment card transaction made on the Visa and MasterCard Networks has multiple moving parts and is handled by several different parties. The transaction is initiated by a merchant (here, Target), electronically sent to the acquiring bank, processed by a payment card transaction processor (*i.e.*, an entity retained by the acquiring bank to actually process the transaction), and authorized by the payment card issuer (here, Plaintiffs and Class Members).

21. When a payment card purchase is made on the Visa Network,[3] the merchant seeks

[3] Transactions made on the MasterCard Network are identical in all relevant respects. On information and belief, the only difference is that in the MasterCard Network, the merchant

authorization from the issuer, which approves or declines the transaction based on the consumer's payment card limit. If the transaction is approved, the merchant processes the transaction and electronically forwards the receipt directly to the acquiring bank. The acquiring bank then pays the merchant and forwards the final transaction data to the issuer which, in turn, reimburses the acquiring bank. The issuer then posts the charge to the consumer's payment card account, and bills and collects the purchase price from the consumer.

22. In accordance with their respective rules, regulations and operating procedures, Visa and MasterCard monitor their respective Networks for potential fraudulent activity. When fraudulent payment card use is suspected, MasterCard notifies affected issuers through a Security Alert while Visa notifies affected issuers via a "Compromised Account Management Systems Alert," or "CAMS Alert." Upon information and belief, these alerts generally set forth the type of compromised data, the relevant timeframe of the compromise, and a list of payment card numbers that have been exposed.

23. When a consumer makes a payment card purchase at a Target retail store, Target collects sensitive customer information, including the cardholder's name, account number, expiration date, CVV codes, and PIN numbers for debit cards. Target stores this information in its point-of-sale system while electronically transmitting the information to third parties in the Visa and MasterCard Networks to process the transaction for payment. Target also collects and stores mailing addresses, phone numbers, and email addresses.

II. Target knew its point-of-sale system was vulnerable as early as 2007.

24. On August 27, 2007, Dr. Neal Krawetz of Hacker Factor Solutions published a white paper entitled "Point-of-Sale Vulnerabilities" (the "White Paper"). According to the White

---

initially seeks authorization/verification from its acquiring bank, which seeks reimbursement from the issuer.

Paper abstract, point-of-sale systems "provide virtually no security" and few point-of-sale systems "implement best practices for handling sensitive information, such as the Visa standards for credit card management." *Id*. at 4 (http://www.hackerfactor.com/papers/cc-pos-20.pdf).

25. The White Paper also provides a detailed description of a typical point-of-sale system and its components, including "branch servers" and how their vulnerability could result in the compromise of millions of payment card accounts. *See id*. at 10-12.

26. Using Target as an example, the White Paper also prophesies the potential ramifications of a data breach in the Target point-of-sale system, accurately predicting over six years ago that as many as 58 million payment card accounts could be compromised if Target's point-of-sale system was ever compromised. *See id.* at 11-12. Dr. Krawetz observed:

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

Id. at 14 (emphasis added).

27. Dr. Krawetz summarized the vulnerable aspects of point-of-sale architecture, including branch servers, concluding that "[e]ven though other sightings have occasionally surfaced, the February 9th [2006] announcement showed the first big vendor being publicly hit with this problem. This compromise was not the first, it is unlikely to be the last, and it certainly will not be the biggest. It is only a matter of time before a national branch server at a large retailer is compromised." *Id.* at 15.

28. On August 7, 2007, a Target employee responsible for Target's point-of-sale

system acknowledged receipt of the White Paper and requested permission to provide it to other Target employees. The Target employee described Dr. Krawetz suggestions as "good ideas."

29. Thereafter, at least seventeen copies of the White Paper were downloaded to a domain owned by Target, the most recent download occurring in May 2013. The search term "POS vulnerability" was used by Target sources to download the White Paper. On information and belief, Target did not heed the White Paper and/or implement any of its suggestions.

III. Target also knew its internal computer network and point-of-sale system was not PCI DSS compliant.

30. Target recognizes its customers' personal and financial information is highly confidential and must be protected. According to Target's December 2013 Privacy Policy, for example, "[b]y interacting with Target, [customers] consent to use of information that is collected or submitted as described in this privacy policy." Target further represents "[w]e maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information." *Id.*

31. The PCI DSS is the industry standard for large retail institutions that accept payment cards. The PCI DSS consists of twelve general standards, including: (i) installing and maintaining firewall(s) to protect data, (ii) protecting stored data, (iii) encrypting the transmission of payment cardholder data and sensitive information across public networks, (iv) using and regularly updating antivirus software, (v) developing and maintaining secure systems and applications, (vi) restricting physical access to cardholder data, (vii) tracking and monitoring all access to network resources and cardholder data, (viii) regularly testing security systems and processes, and (ix) maintaining a policy that addresses information security.

32. The purpose of PCI DSS is to "[b]uild and maintain a secure network; protect

cardholder data; ensure the maintenance of vulnerability management programs; implement strong access control measures; regularly monitor and test networks; and ensure the maintenance of information security policies." *See* www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

33. USA Today, among other sources, however, reported Target was likely not PCI DSS compliant because "the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days." *See* http://www.usatoday.com/story/cybertruth/2013/12/23/qa-pci-rules-could-help-stymie-target- data-thieves/4179941/.

34. Under PCI DSS, merchants like Target are required to encrypt "track data." According to Informationweek.com, the Target Data Breach should never have happened. *See* http://www.informationweek.com/security/attacks-and-breaches/target-breach-10-facts/d/d-id/1113228. Forrester analyst John Kindervag further opined that "[t]he fact that the three-digit CVV security codes were compromised shows they were being stored. Storing CVV codes has long been banned by the card brands and the PCI [Security Standards Council]." *Id.*

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

IV. The Target Data Breach.

36. On December 19, 2013—over a week after Target was first contacted by the Secret Service and four days after confirming the Data Breach, in fact, had occurred—Target announced to the world that hackers had injected malware into its point-of-sale system within its

internal network and stolen sensitive data and information contained on the magnetic stripes of 40 million payment cards, including customer names, credit or debit card numbers, expiration dates, CVV codes, and PIN numbers (*i.e.*, "track data")—thereby giving fraudsters the data necessary to create fake credit cards to make fraudulent purchases and fake debit cards to withdraw cash from the bank accounts of unsuspecting victims.

37. The hackers gained access to Target's point-of-sale system within its internal computer network of systems through Fazio Mechanical Services, Inc., a Pittsburgh based refrigeration contractor, that Target allowed to link remotely to Target's internal computer network of systems for purposes of electronic billing, contract submission and project management. Fazio Mechanical Services installs and maintains refrigerators for supermarket chains and other companies, including BJ's Wholesale Club, Costco, Supervalu, Trader Joe's and Wal-Mart. Target, however, is Fazio Mechanical Services' only customer that gives Fazio access to its internal computer network of systems to remotely manage these processes.

38. The Target Data Breach began on November 27, 2013, as shoppers prepared to swarm Target's 1,800 United States stores to snag Black Friday deals. The malware transmitted the first payload of stolen payment card information to a hijacked internal Target network server on December 2, 2013, which was later downloaded via the Internet in Russia. The malware repeated this process numerous times over the next two weeks.

39. Shortly thereafter, the Secret Service, which is charged with protecting the country's financial infrastructure and payment systems as well as the president, noticed a flood of new stolen payment cards entering the market—a quarter-million to a half-million at a time, which is substantially more than usual—and bought some of them. The Secret Service contacted Target about the fraudulent activity several days before December 15, 2013, whereupon Target

commenced an internal investigation leading up to its December 19, 2013 public announcement.

40. At about the same time, payment card processors also detected a surge in fraudulent transactions involving payment cards used at Target. The *New York Times* reported that as early as December 11, 2013, fraud analysts detected "a ten to twentyfold increase in the number of high-value stolen cards on black market websites, from nearly every bank and credit union." *See* Elizabeth A. Harris, *Target Breach Affected Up to 110 Million Customers*, N.Y. TIMES, Jan. 10, 2014.

41. Prior to being contacted by the Secret Service, Target was not aware of the Data Breach. After being contacted by the Secret Service, Target began working with the Secret Service and Department of Justice to further investigate the Breach. *See* Anne D'Innocenzio, *Target: Justice Dept. Investigates Data Breach*, USA TODAY, Dec. 23, 2013.

42. The compromised payment cards were used by shoppers who visited Target stores from November 27, 2013 through December 15, 2013. On information and belief, Visa, MasterCard, American Express and Discover branded payment cards, as well as Target's REDcard private label payment cards, were affected. KrebsOnSecurity, a closely watched security blog that broke the news of the Target Data Breach on December 18, 2013, reported that the Breach involved nearly all of the Target stores in the United States. Target claims its online business, Target.com, was not impacted. Time will tell.

43. Although Target initially did not disclose how its point-of-sale system was compromised, the WALL STREET JOURNAL reported:

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

See Sara Germano, *Target Faces Backlash after 20-Day Security Breach: Retailer Says 40*

Million Accounts May Have Been Affected Between Nov. 27 and Dec. 15, THE WALL STREET JOURNAL, Dec. 19, 2013.

44. Most experts believe the injected malware was software known as Reedum (also known as Kaptoxa, a Russian slang word for potato), a variant of the BlackPOS malware specifically developed to attack point-of-sale systems.

45. The Reedum malware worked like a Trojan horse by hiding its malicious nature and compromising Target's point-of-sale system from the inside. Once injected into the point-of-sale system, the software sought out and monitored payment programs for the data on payment cards magnetic stripes (*i.e.*, track data) which, during the authorization process, was unencrypted and stored in the point-of-sale system's memory. The data was then scraped and stashed inside a hijacked Target server during the prime business hours of 10 a.m. to 5 p.m., allowing it to blend in with normal traffic. The hackers later harvested the stolen payment card information from the Target server by sending it over the Internet to a computer in Russia.

46. After learning about the Target Data Breach, Plaintiffs and Class Members took certain steps to limit their losses—including cancelling and reissuing the compromised payment cards. On December 21, 2013, for example, J.P. Morgan Chase placed daily limits on debit card use by consumers who shopped at Target. Daily cash withdrawals were limited to $100 with a $300 daily limit on purchases. Holiday shoppers were furious and vocal, taking their complaints to social media. *See* Sara Germano and Dan Fitzpatrick, *J.P. Morgan Chase Places Limits on Debit Cards Used During Target Breach: Caps Placed on Cash Withdrawals and Daily Purchases from Affected Accounts for Now*, THE WALL STREET JOURNAL, Dec. 21, 2013. Two days later, J.P. Morgan Chase eased back on the limitations, allowing its customers to withdraw $250 from ATMs and make $1000 of daily debit card purchases. *See* Sara Germano and Robin

Sidel, *Target Discusses Breach with State Attorneys: Retailer Updates Officials on Investigation,* THE WALL STREET JOURNAL, Dec. 23, 2013.

47. Although Target initially reported PIN numbers pertaining to the stolen debit cards had not been stolen, Target changed its story on December 27, 2013, admitting PIN numbers were also taken during the Breach.

48. KrebsOnSecurity.com reported that payment cards stolen and compromised in the Target Data Breach have flooded underground black markets, selling in batches of one million cards priced from $20 to more than $100 per card. Some financial institutions reportedly purchased large blocks of their own payment card accounts from illicit online "card shops" in an effort to mitigate their losses. *Debit and credit cards stolen in Target breach reportedly for sale in underground black markets* (Fox News television broadcast Dec. 22, 2013).

49. One stolen payment card shop is well known for selling quality "dumps" (*i.e.*, track data stolen from the magnetic stripes on the back of payment cards). The stolen track data allows thieves to clone credit cards to make fraudulent purchases in stores and debit cards to withdraw cash from unsuspecting victims' bank accounts via ATMs.

50. Indeed, shortly after the Target Data Breach began, one card shop proprietor nicknamed *"Rescator,"* who also is a key figure on *"Lampeduza,"* a Russian-language cybercrime forum, began advertising a new base of one million payment cards, dubbed "Tortuga." *See Cards Stolen in Target Breach Flood Underground Markets*, KREBS ON SECURITY, Dec. 20, 2013, https://krebsonsecurity.com/2013/12/whos-selling-credit-cards-from-target/. "Tortuga" is Spanish for tortoise, and the name of a notorious pirate island referenced by Jack Sparrow in the movie "Pirates of the Caribbean." Tortuga is also a near anagram for Target.

51. KrebsOnSecurity was asked by a small issuer bank to help recover (through

online purchase) the bank's credit card accounts compromised by the Data Breach. *Id.* The first step was to determine if the bank's cards were, in fact, being offered for sale via the illicit card shop's website – described as *"remarkably efficient and customer friendly." Id.* Like other card shops, this store allows customers to search for available payment cards using a number of parameters, including the BIN (a bank's unique number, which is the first six digits of a payment card), type of payment card (*e.g.*, MasterCard, Visa, etc.), expiration date, track type, country and/or the name of the financial institution that issued the card. *Id.* Payment cards stolen and compromised in the Target Data Breach were identified in the store as a mix of MasterCard dumps ranging in price from $26.60 to $44.80 apiece. *Id.*

52. As an additional service, the card shop also provides purchasers with the ZIP code and city location of the Target store from which the payment card information was stolen. *Id.* This information is valuable to fraudsters because they will make same-state purchases, thereby avoiding any knee-jerk fraud defenses a financial institution might use to block out-of-state transactions from a known compromised payment card. *Id.*

53. The issuer bank quickly ran fraud and common point-of-purchase analyses on each of the dumps it purchased that confirmed all of the stolen and repurchased payment cards had been used to make purchases at Target stores between November 29, 2013 and December 15, 2013. *Id.* Some payment cards had already been tagged "confirmed fraud," while others were only recently issued and had only been used at Target. *Id.* KebsOnSecurity and the bank also discovered that a number of the stolen and repurchased payment cards were flagged for fraud after the Target Data Breach because they were used to make unauthorized purchases at big box retailers, *"including – wait for it – Target." Id.*

54. According to the Consumer Bankers Association ("CBA"), to date, the Breach

has cost its U.S. member banks over $172 million just to re-issue the stolen payment cards. *See* http://www.finextra.com/news/fullstory.aspx?newsitemid=25702&topic=payments. This number does not include fraudulent purchases and/or unauthorized cash withdrawals the banks have also absorbed. Specifically regarding the Target Data Breach, Richard Hunt, President and CEO of the CBA, opined:

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

Id. A recent analysis by Jefferies, the global investment banking firm, suggests that payment card issuers could sustain upwards of $1 billion of damages as a result of the Target Data Breach based on an estimated 4.8 million to 7.2 million of the stolen and compromised payment cards being used to make fraudulent purchases and/or unauthorized cash withdrawals. *Id.*

55. On January 10, 2014, Target subsequently revealed, for the first time, that PII of an additional 70 million individuals was also stolen in the Breach. The stolen PII includes customer names, mailing addresses, phone numbers and/or email addresses.

V. The Target Data Breach never should have happened.

56. The Target Data Breach was preventable. Target knew its data security policies, procedures, protocols, and hardware and software systems were insufficient, antiquated, and did not safeguard and protect sensitive consumer data from theft, yet did nothing to expand, improve and/or update them.

57. In addition to implementing Dr. Krawetz' White Paper suggestions and bringing its internal computer network and point-of-sale system into compliance with PCI DSS, the Data Breach would have been prevented had Target instituted an effective Enterprise Risk

Management ("ERM") system supported by the appropriate ERM software. With an effective ERM process, the risk of a data breach would have been documented and assessed in a way that would have provided transparency to Target senior management who, in turn, would have had the time and opportunity to take steps to prevent the Data Breach before it occurred. Even for an entity the size of Target, a fully developed ERM system would have cost Target substantially less than 3% of the estimated cost of the Target Data Breach.[4] On information and belief, however, Target failed and refused to develop and implement an effective ERM system—much less, an ERM system of any kind.

58. The Target Data Breach also would have been prevented had Target installed the appropriate antivirus software in its point-of-sale system and across its entire internal network. Several readily available antivirus software programs—such as AVG, Bitdefender and ThreatTrack—would have detected and removed the malware used by the hackers. On information and belief, however, Target failed and refused to install the appropriate antivirus software in its point-of-sale system and/or across its entire internal computer network.

59. The Target Data Breach also would have been prevented had Target set the policies on its local store computers in its point-of-sale system to disable the installation of malware such that its installation would have been impossible. On information and belief, however, Target failed and refused to set the policies on its local store computers in its point-of-sale system to disable the installation of malware.

60. The Target Data Breach also would have been prevented had Target implemented

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

basic security measures related to authentication; specifically, two- factor authentication on its point-of-sale terminals for anyone attempting to remotely connect to them. On information and belief, however, Target failed and refused to implement these authentication-based basic security measures on its point-of-sale terminals.

61. The Target Data Breach also would have been prevented had Target properly monitored its point-of-sale system for signs of attack. On information and belief, however, Target failed and refused to properly monitor its point-of-sale system.

62. The Target Data Breach also would have been prevented had Target disconnected its point-of-sale system from the Internet. There is no reason for point-of-sale terminals to be freely accessible via the Internet. At the very least, outbound access to the Internet by the point-of-sale system should have been blocked by a firewall, which would have prevented the stolen payment card information from being uploaded to the Internet and transmitted to Russia.

63. The key to effective data security is layered security—which Target did not have in place. Had layered data security been in place, the data thieves would have first had to determine how to deploy the malware, and then determine how to circumvent the antivirus software running on the point-of-sale terminals. Even if they could have accomplished these feats—which they would not have been able to do—the malware would have been blocked by the firewall or network segmentation when trying to access the Internet. Had Target taken even the most fundamental layered data security measures, the Breach would not have happened.

VI. Target has accepted full responsibility for the Data Breach.

64. In a January 13, 2014 interview with CNBC's Becky Quick, Gregg Steinhafel ("Steinhafel"), Target's Chairman, CEO and President, stated "clearly, we're accountable and we're responsible" for the Data Breach, and "we're going to make significant changes."

65. Steinhafel is currently pushing for new payment card technology for American consumers, a chip-and-PIN-number system (also known as EMV technology), that replaces vulnerable magnetic stripes on payment cards. Hackers find it increasingly easy to steal and use the data on magnetic stripe payment cards for two key reasons—the sensitive cardholder information in the payment stripe does not change and fake payment cards can be easily cloned with readily available technology. Chip cards, on the other hand, convert sensitive cardholder information into a unique code for each transaction, and often require additional authentication, such as a PIN number. As an example of their effectiveness, adoption of the chip cards in Great Britain reduced counterfeit payment card fraud by 70% between 2007 and 2012. By contrast, data breaches at United States retailers more than doubled during the same time period.

66. Although progress is being made in the United States regarding the adoption and use of chip cards—the current target date in late 2015—industry experts believe momentum, in fact, was substantially impeded by Target following its failed 2001-2004 collaboration with Visa to use chip cards in Target stores. Ironically, Target had the opportunity to be the industry leader, but Target executives responsible for store operations and merchandising—led by Steinhafel—killed the chip card program because the technology slowed checkout speeds and did not offer Target enough marketing benefits. Checkout speed and marketing benefits were (and continue to be) more important to Target than the security of its customers' sensitive payment card information and PII. Steinhafel's resurrected infatuation with chip card technology in the wake of the Data Breach rings hollow.

67. Target has repeatedly pledged that no consumer will sustain any damages as a result of the Target Data Breach, touting its one year free offer of single bureau credit monitoring services (Experian ProtectMyID) to affected customers. According to *Consumer Reports*,

however, Target "fumbled" when it offered this "second-rate credit-monitoring service." At best, the ProtectMyID credit monitoring service is an indirect manner of tracking identity theft—it may reveal new credit accounts opened with the stolen information, but does nothing to monitor unauthorized charges made to existing payment card accounts. *See Consumer Reports Calls Target's Response to Data Breach Weak,* UPI, Feb. 6, 2014, http://www.upi.com/Business_News/2014/02/06/Consumer-Reports-calls-Targets-response-to-data-breach-weak/UPI-69291391732657/print#ixzz2sflHce3T.

68. The three large credit bureaus—Experian, Equifax and TransUnion—also can produce very different reports, so the use of only one credit bureau monitoring service, Experian, is an inefficient monitoring strategy. *Id.* Moreover, once a credit monitoring system begins to warn a consumer of suspicious activity on an account, the warnings pile up so quickly consumers frequently begin to ignore the alerts. *Id.* Finally, after affected consumers sign up for the program, Experian, seizing a golden opportunity to push other products and services, will bombard them with advertising to sell them various credit reports for a fee—including the three bureau credit monitoring service Target decided not to offer. *Id.* "Some of these Experian ads exploit consumers who are ignorant of their rights because consumer protection laws allow [identity] theft victims to place a free 90-day fraud alert on their credit reports and get their credit reports from all three credit bureaus absolutely free." *Id.*

69. While Target has thrown consumers somewhat of a bone in an effort to rebuild customer loyalty, improve its financial outlook, and stem the hemorrhaging of its stock price (Target has lost more than $10 billion of its market cap since July 2013), Target has not offered Plaintiffs and Class Members any compensation for the hard damages they have incurred (and will continue to incur) in the form, *inter alia*, expenses to cancel and reissue the stolen and compromised payment cards and the absorption of fraudulent charges made on the compromised

payment cards.

TARGET'S PATTERN OF UNLAWFUL ACTIVITY UNDER 18 U.S.C. § 1961, *et seq.*: INTERSTATE AND/OR FOREIGN WIRE FRAUD

70. The preceding factual statements and allegations are incorporated by reference.

71. Target knew, and intentionally so acted, that Plaintiffs and Class Members are part of the Visa and MasterCard Networks and rely on merchants that accept Visa and MasterCard payment cards to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems—especially in point-of-sale systems. Target, however, intentionally devised, engaged in, condoned and/or ratified the above-described open-ended, unlawful and schemes to (i) defraud and cheat Plaintiffs and Class Members to obtain money, funds, credits, assets, and/or other property owned by, or under the custody or control of, Plaintiffs and Class Members by means of false or fraudulent pretenses and/or (ii) fraudulently and intentionally misrepresent to Plaintiffs and Class Members—explicitly and/or implicitly—through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate and/or foreign wires, its website, and its participation in the Visa and MasterCard Networks that (a) it was in compliance with the Visa Operating Regulations and/or MasterCard Rules mandating the protection of payment card information and prohibiting the retention or storage of payment card account numbers, PIN numbers, personal information, magnetic stripe information, and/or transaction information subsequent to the approval of the transaction, (b) it was in compliance with the PCI DSS, and (c) its customer data security policies, procedures, protocols, and hardware and software systems were in place and would safeguard and protect sensitive customer data—including the stolen and compromised payment card information—for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Target and/or approve millions of

payment card purchases made at Target via the interstate and/or foreign wires for the further purpose of increasing Target's revenue, profitability, and return on investment. Alternatively, Target fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse was true. By doing so, Target (i) directly and/or proximately caused Plaintiffs and Class Members to suffer damages to their businesses and/or property, (ii) saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (iii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members. Target intentionally engaged in these wrongful actions, inaction and/or omissions for its financial benefit and to Plaintiffs' and Class Members' financial detriment.

72. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions wrongfully cheated Plaintiffs and Class Members and violated all concepts of moral uprightness, fundamental honesty, fair play and right dealing in the general and business life of the members of society. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions also unfairly betrayed the confidences Plaintiffs and Class Members placed in Target. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions also were a consistent, regular and dominant part of the manner in which it participated in, and conducted its day-to-day business dealings with, Plaintiffs, Class Members and other members of the Visa and MasterCard Networks (the RICO enterprises).

73. Target intentionally devised, instigated, perpetrated, executed, condoned and/or ratified the above-described schemes by means of false or fraudulent pretenses, and engaged in the above-described repeated and systematic interstate and/or foreign wire fraud, by using and/or causing the use of the interstate and/or foreign wires to (i) secure the authorization of millions of

payment card transactions from Plaintiffs and Class Members, each of which was a separate violation of 18 U.S.C. § 1343, and (ii) post to and maintain its website and participate in the Visa and MasterCard Networks, each transaction of which also was a separate violation of 18 U.S.C. § 1343.

74. Target used and/or caused the Visa and MasterCard Networks (the RICO enterprises) to use the interstate and/or foreign wires in interstate and/or foreign commerce to devise, engage in, condone and/or ratify the above-described open-ended, unlawful and intentional schemes by means of false or fraudulent pretenses, representations and/or promises through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate and/or foreign wires, its website, and its participation in the Visa and MasterCard Networks, without the knowledge or approval of Plaintiffs and Class Members, for the purposes of increasing Target's revenue, profitability, and return on investment. The dates and substance of Target's schemes and/or internal and external fraudulent communications, via the interstate and/or foreign wires, in furtherance of the above-described schemes, as well as their fraudulent communications to Plaintiffs and Class Members, via the interstate and/or foreign wires, in furtherance of their above-described schemes are in Target's possession, custody, and control, and await discovery. By its unlawful actions, inaction and/or omissions, Target (i) conducted and/or participated in the affairs of the Visa Network and MasterCard Network (the RICO enterprises) (in violation of 18 U.S.C. § 1962(c)), and/or (ii) conspired to violate 18 U.S.C. § 1962 (a) and (c) (in violation of 18 U.S.C. § 1962(d)), and defrauded Plaintiffs and Class Members in the process.

75. Target caused the Visa and MasterCard Networks (the RICO enterprises) to engage in the above-described open-ended, unlawful, intentional and fraudulent schemes—without Plaintiffs' and Class Members' knowledge or approval—for the purpose of increasing

Target's revenue, profitability, and return on investment to the financial detriment of Plaintiffs and Class Members. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions constitute interstate and/or foreign wire fraud in violation of 18 U.S.C. § 1343.

76. Target's above-described multiple, repeated and continuous acts of interstate and/or foreign wire fraud constitute a pattern of unlawful activity under to 18 U.S.C. § 1961(1); (5). Nothing in the nature of the above-described open-ended, unlawful, intentional and fraudulent schemes demonstrates that Target's unlawful and intentional schemes, wrongful actions, inaction and/or omissions would ever have terminated but for this Court's intervention. Moreover, and independent of the duration of the schemes, Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions were a consistent, regular and dominant part of the manner in which it conducted and/or participated in the day-to-day business and financial affairs of the Visa Network and MasterCard Network (the RICO enterprises).

CLASS ACTION ALLEGATIONS

77. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action against Target as a national class action, for themselves and all members of the following Class of similarly situated payment card issuers:

> All banks, credit unions, financial institutions and other entities that (i) issued Visa and/or MasterCard branded credit cards and/or debit cards that were stolen and compromised by the Target Data Breach, (ii) cancelled and re-issued the compromised payment cards, and/or (iii) absorbed unauthorized charges made on the compromised payment cards.

78. The proposed Class consists of hundreds, if not thousands, of geographically dispersed members, the joinder of which in one action is impracticable. The precise number and identities of the Class Members are currently unknown to Plaintiffs, but can easily be derived

from the list of stolen and compromised payment cards Target has already compiled, and their issuers, which Target, Visa and/or MasterCard have already notified.

79. Target violated the rights of each Class Member in the same way by its above-described uniform unlawful and intentional schemes, wrongful actions, inaction and/or omissions.

80. There are questions of law and fact common to the proposed Class as a whole that predominate over any questions affecting individual Class Members including, *inter alia*:

(i) whether Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions violated 18 U.S.C. § 1962(c) and/or (d);

(ii) whether Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions constitute negligent misrepresentation at common law;

(iii) whether Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions constitute negligence/gross negligence at common law;

(iv) whether Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions constitute negligence *per se* at common law;

(v) whether Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions constitute breach of contract at common law;

(vi) whether Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions constitute unfair and deceptive acts and practices in violation of Minn. Stat. § 325F.69, subd. 1;

(vii) whether Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions violated Minn. Stat. § 325E.64;

(viii) whether Target should be compelled to refund (or disgorge) the amounts by which it has been unjustly enriched and/or compelled to make restitution under the common law equitable doctrine of assumpsit;

(ix) whether Target's above-described wrongful unlawful and intentional schemes, wrongful actions, inaction and/or omissions directly and/or proximately caused Plaintiff and Class Members to suffer damages;

(x) whether Plaintiffs and Class Members are entitled to recover actual damages,

consequential damages, incidental damages, statutory damages, punitive damages, RICO treble damages, pre- and post-judgment interest, attorneys' fees, litigation expenses and/or court costs and, if so, the amount of the recovery; and

(xi) whether Plaintiffs and Class Members are entitled to injunctive relief.

81. Plaintiffs' claims are typical of Class Members' claims because Plaintiffs and Class Members are all victims of Target's above-described schemes to cheat and defraud them by means of false or fraudulent pretenses, representations, or promises.

82. Plaintiffs and their counsel will fairly and adequately represent the interests of Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, any of the Class Members' interests. Plaintiffs' counsel are highly experienced in leading and prosecuting class actions and complex commercial litigation, including data breach, financial institution and RICO cases.

83. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and Class Members' claims. Plaintiffs and Class Members have been (and will continue to be) harmed as a direct and/or proximate result of Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions. Litigating this case as a class action is appropriate because (i) it will avoid a multiplicity of suits and the corresponding burden on the courts and Parties, (ii) it would be virtually impossible for all Class Members to intervene as parties-plaintiff in this action, (iii) it will allow numerous entities with claims too small to adjudicate on an individual basis because of prohibitive litigation costs to obtain redress for their injuries, and (iv) it will provide court oversight of the claims process once Target's liability is adjudicated.

84. Class Members are readily ascertainable since they have all been notified that certain payment cards issued by them were compromised by the Target Data Breach, whereupon they cancelled and re-issued such compromised payment cards and/or absorbed fraudulent

charges made to the compromised payment cards.

85. Certification, therefore, is appropriate under FED. R. CIV. P. 23(b)(3) because the above-described common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

86. Certification also is appropriate under FED. R. CIV. P. 23(b)(2) because Target has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief and/or equitable relief with respect to the Class as a whole.

87. Certification also is appropriate under FED. R. CIV. P. 23(b)(1) because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Target. For example, one court might decide that the challenged actions are illegal and enjoin Target, while another court might decide that the same actions are not illegal. Individual actions also could be dispositive of the interests of the other Class Members who were not parties to such actions and substantially impair or impede their ability to protect their interests.

88. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions are applicable to the Class as a whole, for which Plaintiffs seek, *inter alia*, damages and equitable remedies.

89. Absent a class action, Target will retain the benefits of its wrongdoing despite seriously violating the law and inflicting substantial harm on Plaintiffs' and Class Members' businesses and property.

CLAIMS FOR RELIEF/ CAUSES OF ACTION

COUNT I

VIOLATIONS OF 18 U.S.C. § 1962(c)

90. The preceding factual statements and allegations are incorporated by reference.

91. Each Plaintiff and each Class Member is a "person" within the meaning of 18 U.S.C. §§ 1961(3), 1964(c).

92. Target is a "person" within the meaning of 18 U.S.C. §§ 1961(3) and 1962(a).

93. The Visa Network and MasterCard Network are "enterprises" within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c) and, at all relevant times, were engaged in, and the activities of which affected, interstate and/or foreign commerce within the meaning of 18 U.S.C. §§ 1961(4), 1962(c), 1962(d).

94. Target conducted and/or participated in the business and financial affairs of the Visa and MasterCard Networks (the RICO enterprises) through a pattern of unlawful activity within the meaning of 18 U.S.C. §§ 1961(1)(B), 1961(5), 1962(c)—to wit, the above-described multiple, repeated, and continuous acts of interstate and/or foreign wire fraud in violation of 18 U.S.C. §§ 2 and 1343.

95. Target's pattern of unlawful activity and corresponding violations of 18 U.S.C. § 1962(c) directly and/or proximately caused Plaintiffs and Class Members to suffer injury to their businesses and/or property within the meaning of 18 U.S.C. § 1964(c)—to wit, Plaintiffs and Class Members were damaged (and will continue to be damaged) by Target engaging in the above-described repeated and systematic interstate and/or foreign wire fraud, in violation of 18 U.S.C. § 1343, to devise, engage in, condone and/or ratify the above-described open-ended, unlawful and intentional schemes to (i) defraud and cheat Plaintiffs and Class Members to obtain money, funds, credits, assets, and/or other property owned by, or under the custody or control of,

Plaintiffs and Class Members by means of false or fraudulent pretenses, and/or (ii) fraudulently and intentionally misrepresent to Plaintiffs and Class Members—explicitly and/or implicitly—through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate and/or foreign wires, its website, and its participation in the Visa Network and MasterCard Network that (a) it was in compliance with the Visa Operating Regulations and/or MasterCard Rules mandating the protection of payment card information and prohibiting the retention or storage of payment card account numbers, PIN numbers, personal information, magnetic stripe information, and/or transaction information subsequent to the approval of the transaction, (b) it was in compliance with the PCI DSS, and (c) its customer data security policies, procedures, protocols, and hardware and software systems were in place and would safeguard and protect sensitive customer data—including the stolen and compromised payment card information—for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Target and/or approve millions of payment card purchases made at Target via the interstate and/or foreign wires for the further purpose of increasing Target's revenue, profitability, and return on investment. Alternatively, Target fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse was true. By doing so, Target (i) directly and/or proximately caused Plaintiffs and Class Members to suffer damages to their businesses and/or property, (ii) saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (iii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members.

96. Plaintiffs and Class Members also were damaged (and will continue to be damaged) by the earnings and profits they would have earned on the funds used to cancel and reissue the compromised payment cards and/or the fraudulent charges made on the compromised

payment cards they absorbed. Target intentionally caused the Visa and MasterCard Networks (the RICO enterprises) to engage in multiple predicate acts of interstate and/or foreign wire fraud to, in turn, engage in the above-described open-ended, unlawful, intentional and fraudulent schemes and commit the above-described substantive RICO offenses by means of false or fraudulent pretenses, representations, or promises—without Plaintiffs' and Class Members' knowledge or approval—for the purpose of increasing Target's revenue, profitability, and return on investment to the financial detriment of Plaintiffs and Class Members.

97. Target knew its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions were fraudulent, misleading and illegal, and would cause Plaintiffs and Class Members to suffer damages in the form of, *inter alia*, the expenses to cancel and reissue compromised payment cards, the absorption of fraudulent charges made on the compromised payment cards, business destruction, lost profits and/or lost business opportunities. All of Plaintiffs' and Class Members' damages were reasonably foreseeable by Target and/or anticipated as a substantial factor and a natural consequence of its pattern of unlawful activity.

COUNT II

VIOLATION OF 18 U.S.C. § 1962(d) BY
CONSPIRING TO VIOLATE 18 U.S.C. § 1962(a)

98. The preceding factual statements and allegations are incorporated by reference.

99. Each Plaintiff and each Class Member is a "person" within the meaning of 18 U.S.C. §§ 1961(3), 1964(c).

100. Target is a "person" within the meaning of 18 U.S.C. §§ 1961(3) and 1962(a).

101. The Visa Network and MasterCard Network are "enterprises" within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c) and, at all relevant times, were engaged in, and the activities of which affected, interstate and/or foreign commerce within the meaning of 18 U.S.C.

§§ 1961(4), 1962(c), 1962(d).

102. On information and belief, Target conspired with other persons and/or entities, the identities of whom are known only to Target at this time, within the meaning of 18 U.S.C. § 1962(d) to violate 18 U.S.C. § 1962(a); that is, Target and its co-conspirators conspired to receive income derived, directly or indirectly, from a pattern of unlawful activity in which Target and its co-conspirators participated as principals within the meaning of 18 U.S.C. §§ 1961(1)(B), 1961(5), and 1962(a)—to wit, the above-described open-ended, unlawful and fraudulent schemes to (i) defraud and cheat Plaintiffs and Class Members to obtain money, funds, credits, assets, and/or other property owned by, or under the custody or control of, Plaintiffs and Class Members by means of false or fraudulent pretenses and/or (ii) fraudulently and intentionally misrepresent to Plaintiffs and Class Members—explicitly and/or implicitly—through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate and/or foreign wires, its website, and its participation in the Visa Network and MasterCard Network that (a) it was in compliance with the Visa Operating Regulations and/or MasterCard Rules mandating the protection of payment card information and prohibiting the retention or storage of payment card account numbers, PIN numbers, personal information, magnetic stripe information, and/or transaction information subsequent to the approval of the transaction, (b) it was in compliance with the PCI DSS, and (c) its customer data security policies, procedures, protocols, and hardware and software systems were in place and would safeguard and protect sensitive customer data—including the stolen and compromised payment card information—for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Target and/or approve millions of payment card purchases made at Target via the interstate and/or foreign wires for the further purpose of increasing Target's revenue, profitability, and return on investment. Alternatively, Target fraudulently and intentionally

failed to disclose to Plaintiffs and Class Members that the reverse was true. Target and its co-conspirators intentionally participated in a conspiracy to engage in the above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions for Target's financial benefit and to Plaintiffs' and Class Members' financial detriment in violation of 18 U.S.C. §§ 2 and 1343. The members, time and place of this complex, multi-party conspiracy are known only by Target at this time and await discovery.

103. Target used or invested (and continues to use or invest), directly or indirectly, such income, or the proceeds of such income, in its ongoing participation in the Visa and MasterCard Networks (the RICO enterprises) and/or the creation and/or operation of one or more other Target-owned stand-alone enterprises including, without limitation, (i) Target.com, which owns and operates Target's e-commerce initiatives, (ii) Financial and Retail Services, which issues the Target-branded payment card known as the REDcard, (iii) Target Sourcing Services, the global sourcing organization that locates, acquires and imports merchandise from around the world for Target and Target.com, (iv) Target Commercial Interiors, which provides design services and furniture for office space for its Fortune 500/1000 business customers, and (v) Target Brands, which owns and oversees Target's trademarks, brands and private label products. All of the above-described stand-alone Target-owned enterprises are engaged in, or the activities of which affect, interstate and/or foreign commerce.

104. The pattern of unlawful activity and corresponding violations of 18 U.S.C. § 1962(d) engaged in by Target and its co-conspirators directly and/or proximately caused Plaintiffs and Class Members to suffer injury to their businesses and/or property within the meaning of 18 U.S.C. § 1964(c)—to wit, Plaintiffs and Class Members were damaged (and will continue to be damaged) in their businesses and/or property in the form of, *inter alia*, expenses to cancel and reissue the stolen and compromised payment cards and the absorption of fraudulent

charges made on the compromised payment cards by means of false or fraudulent pretenses, representations, or promises by engaging in the above-described repeated and systematic interstate and/or foreign wire fraud by using and/or causing the use of the interstate and/or foreign wires to (i) secure the authorization of millions of payment card transactions from Plaintiffs and Class Members via the interstate and/or foreign wires, each of which was a separate violation of 18 U.S.C. § 1343, and (ii) post to and maintain its website and participate in the Visa and MasterCard Networks, each transaction of which also was a separate violation of 18 U.S.C. § 1343. Plaintiffs and Class Members also were damaged (and will continue to be damaged) by the earnings and profits they would have earned on the funds used to cancel and reissue the compromised payment cards and/or the fraudulent charges made on the compromised payment cards Plaintiffs and Class Members absorbed.

105. Target and its co-conspirators caused the Visa and MasterCard Networks (the RICO enterprises) to engage in the above-described multiple predicate acts of interstate and/or foreign wire fraud to, in turn, engage in the above-described open-ended, unlawful, intentional and fraudulent schemes and commit the above-described substantive RICO offenses by means of false or fraudulent pretenses, representations, or promises—without Plaintiffs' and Class Members' knowledge or approval—for the purpose of increasing Target's revenue, profitability, and return on investment to the financial detriment of Plaintiffs and Class Members.

106. Target knew its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions were fraudulent, misleading and illegal, and would cause Plaintiffs and Class Members to suffer the above-described damages. All of Plaintiffs' and Class Members' damages were reasonably foreseeable by Target and/or anticipated as a substantial factor and a natural consequence of its pattern of unlawful activity.

COUNT III

VIOLATION OF 18 U.S.C. § 1962(d) BY CONSPIRING TO VIOLATE 18 U.S.C. § 1962(c)

107. The preceding factual statements and allegations are incorporated by reference.

108. Plaintiffs and Class Members are "persons" within the meaning of 18 U.S.C. §§ 1961(3), 1964(c).

109. Target is a "person" within the meaning of 18 U.S.C. §§ 1961(3) and 1962(a).

110. The Visa Network and MasterCard Network are "enterprises" within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c) and, at all relevant times, were engaged in, and the activities of which affected, interstate and/or foreign commerce within the meaning of 18 U.S.C. §§ 1961(4), 1962(c), 1962(d).

111. On information and belief, Target conspired with other persons and/or entities, the identities of whom are known only to Target at this time, within the meaning of 18 U.S.C. § 1962(d) to violate 18 U.S.C. § 1962(c); that is, Target and its co-conspirators conspired to conduct and/or participate in the business and financial affairs of the Visa and MasterCard Networks (the RICO enterprises) through a pattern of unlawful activity within the meaning of 18 U.S.C. §§ 1961(1)(B), 1961(5), and 1962(c)—to wit, the above-described open-ended, unlawful and fraudulent schemes to (i) defraud and cheat Plaintiffs and Class Members to obtain money, funds, credits, assets, and/or other property owned by, or under the custody or control of, Plaintiffs and Class Members by means of false or fraudulent pretenses and/or (ii) fraudulently and intentionally misrepresent to Plaintiffs and Class Members—explicitly and/or implicitly—through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate and/or foreign wires, its website, and its participation in the Visa Network and MasterCard Network that (a) it was in compliance with the Visa Operating

Regulations and/or MasterCard Rules mandating the protection of payment card information and prohibiting the retention or storage of payment card account numbers, PIN numbers, personal information, magnetic stripe information, and/or transaction information subsequent to the approval of the transaction, (b) it was in compliance with the PCI DSS, and (c) its customer data security policies, procedures, protocols, and hardware and software systems were in place and would safeguard and protect sensitive customer data—including the stolen and compromised payment card information—for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Target and/or approve millions of payment card purchases made at Target via the interstate and/or foreign wires for the further purpose of increasing Target's revenue, profitability, and return on investment. Alternatively, Target fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse was true. Target and its co-conspirators intentionally participated in a conspiracy to engage in the above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions for Target's financial benefit and to Plaintiffs' and Class Members' financial detriment. in violation of 18 U.S.C. §§ 2 and 1343. The members, time and place of this complex, multi-party conspiracy are known only by Target at this time and await discovery.

112. The pattern of unlawful activity and corresponding violations of 18 U.S.C. § 1962(d) engaged in by Target and its co-conspirators directly and/or proximately caused Plaintiffs and Class Members to suffer injury to their businesses and/or property within the meaning of 18 U.S.C. § 1964(c)—to wit, Plaintiffs and Class Members were damaged (and will continue to be damaged) in their businesses and/or property in the form of, *inter alia*, expenses to cancel and reissue the stolen and compromised payment cards and the absorption of fraudulent charges made on the compromised payment cards by means of false or fraudulent pretenses, representations, or promises by engaging in the above-described repeated and systematic

interstate and/or foreign wire fraud by using and/or causing the use of the interstate and/or foreign wires to (i) secure the authorization of millions of payment card transactions from Plaintiffs and Class Members via the interstate and/or foreign wires, each of which was a separate violation of 18 U.S.C. § 1343, and (ii) post to and maintain its website and participate in the Visa and MasterCard Networks, each transaction of which also was a separate violation of 18 U.S.C. § 1343. Plaintiffs and Class Members also were damaged (and will continue to be damaged) by the earnings and profits they would have earned on the funds used to cancel and reissue the compromised payment cards and/or the fraudulent charges made on the compromised payment cards Plaintiffs and Class Members absorbed.

113. Target and its co-conspirators caused the Visa and MasterCard Networks (the RICO enterprises) to engage in the above-described multiple predicate acts of interstate and/or foreign wire fraud to, in turn, engage in the above-described open-ended, unlawful, intentional and fraudulent schemes and commit the above-described substantive RICO offenses by means of false or fraudulent pretenses, representations, or promises—without Plaintiffs' and Class Members' knowledge or approval—for the purpose of increasing Target's revenue, profitability, and return on investment to the financial detriment of Plaintiffs and Class Members.

114. Target knew its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions were fraudulent, misleading and illegal, and would cause Plaintiffs and Class Members to suffer the above-described damages. All of Plaintiffs' and Class Members' damages were reasonably foreseeable by Target and/or anticipated as a substantial factor and a natural consequence of its pattern of unlawful activity.

COUNT IV

NEGLIGENT MISREPRESENTATION

115. The preceding factual statements and allegations are incorporated by reference.

116. By its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions, Target negligently failed to disclose to Plaintiffs and Class Members the material and important facts that (i) it was not in compliance with the Visa Operating Regulations and MasterCard Rules mandating the protection of payment card information and prohibiting the retention or storage of payment card account numbers, personal information, magnetic stripe information, and/or transaction information subsequent to the approval of the transaction, (ii) it was not in compliance with the PCI DSS, and (iii) its customer data security policies, procedures, protocols, and hardware and software systems would not safeguard and protect sensitive customer data—including the payment card information stolen and compromised in the Target Data Breach. Target's material omissions were made in the course of Target's business for the guidance of Plaintiffs and Class Members in their business transactions with Target, including issuing payment cards used to make purchases at Target and/or approving millions of payment card purchases made at Target via the interstate and/or foreign wires. As set forth above, Target also negligently made incorrect statements concerning its customer data security policies, procedures, protocols, and hardware and software systems, falsely communicating material facts.

117. Target knew that Plaintiffs and Class Members are part of the Visa and MasterCard Networks and rely on merchants that accept Visa and MasterCard payment cards to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems—especially in their point-of-sale systems.

118. Target failed to exercise reasonable care or competence in withholding this information the truth from Plaintiffs and Class Members; to wit, the material and important fact that its customer data security policies, procedures, protocols, and hardware and software systems, in fact, did not safeguard and protect sensitive customer data—including the payment card information stolen and compromised in the Target Data Breach.

119. Plaintiffs and Class Members justifiably relied on Target's silence and incorrect statements, when Target had a duty to speak, which directly and/or proximately caused Plaintiffs and Class Members to suffer injury to their businesses and/or property including, *inter alia*, the expenses to cancel and reissue compromised payment cards, the absorption of fraudulent charges made on the compromised payment cards, business destruction, lost profits and/or lost business opportunities. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions constitute negligent misrepresentation at common law.

COUNT V

NEGLIGENCE/GROSS NEGLIGENCE

120. The preceding factual statements and allegations are incorporated by reference.

121. Upon coming into possession of the private, non-public, sensitive payment card information and PII of Plaintiffs' and Class Members' customers, Target had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the payment card information and PII from being stolen and/or compromised. Target's duty arises from the common law, in part, because it was reasonably foreseeable to Target under the circumstances

that a data breach in its point-of-sale system was likely to occur that would cause Plaintiffs' and Class Members' above-described damages, as well as from the duties expressly imposed upon Target from other sources, such as compliance with industry standards (*i.e.*, PCI DSS), implied contracts between Target and Plaintiffs and Class Members, contracts between Target and other third parties (such as its acquiring bank), and participation in the Visa and MasterCard Networks (and the corresponding Visa Operating Regulations and MasterCard Rules).

122. Target also had a duty to timely disclose to Plaintiffs, Class Members, and their customers that the Data Breach had occurred and the private, non-public, sensitive payment card information and PII of Plaintiffs' and Class Members' customers had been stolen and compromised—at least so that Plaintiffs, Class Members, and their customers could take the appropriate steps necessary to minimize their damages. Instead, by its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions, and delayed disclosure of the Data Breach, Target shifted its notification obligation and expenses to Plaintiffs and Class Members. Target also (i) directly and/or proximately caused Plaintiffs and Class Members to suffer the above-described damages to their businesses and/or property, (ii) saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (iii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members. Target's duty to properly and timely disclose the Data Breach to Plaintiffs, Class Members, and their customers also arises from the same above-described sources.

123. Target also had a duty to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems—especially in its point-of-sale systems—to prevent and detect data breaches and the unauthorized dissemination of Plaintiffs' and Class Members' customers' private, non-public, sensitive financial information—

including the payment card information and PII stolen and compromised by the Target Data Breach. Such duty also arises from the same above-described sources.Target, by and through its above-described negligent and/or grossly negligent actions, inaction, omissions and/or silence when it had a duty to speak, unlawfully breached its duties to Plaintiffs and Class Members by, *inter alia*, failing to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems—especially in its point-of-sale system—granting at least one outside vendor access to its internal computer network of systems through which the malware was placed inside Target's point-of-sale system, and failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' customers' private, non-public, sensitive payment card information and PII that was within Target's possession, custody and control.

124. Target, by and through its above-described negligent and/or grossly negligent actions, inaction, omissions and/or silence when it had a duty to speak, unlawfully also breached its duties to Plaintiffs, Class Members and their customers to properly and timely notify them of the Data Breach so they could take the necessary steps to minimize their damages. But for Target's grossly negligent, negligent and/or wrongful breach of the duties it owed (and continues to owe) Plaintiffs and Class Members, their customers' private, non-public, sensitive payment card information and PII would never have been stolen and compromised, the Data Breach would not have occurred, and Plaintiffs and Class Members would not have incurred damages notifying their customers about the Target Data Breach, canceling and reissuing the compromised payment cards, and/or absorbing unauthorized charges made on the compromised payment cards.

125. The Target Data Breach and the above-described substantial injuries suffered by Plaintiffs and Class Members as a direct and/or proximate result of the Data Breach were reasonably foreseeable consequences of Target's negligence and/or gross negligence.

126. The economic loss doctrine does not apply to bar Plaintiffs' and Class Members' negligence and/or gross negligence claims because, *inter alia*, (i) Target is in the business of supplying information for the guidance of Plaintiffs and Class Members regarding its business transactions (*i.e.*, its electronic payment card transactions for which it regularly seeks authorization from Plaintiffs and Class Members via the interstate and/or foreign wires to consummate), (ii) Target made the above-described negligent and/or grossly negligent misrepresentations, and/or engaged in the above-described negligent and/or grossly negligent conduct, and (iii) Plaintiffs and Class Members are not in direct privity of contract with Target.

COUNT VI

NEGLIGENCE *PER SE*

127. The preceding factual statements and allegations are incorporated by reference.

128. At all relevant times, Target was required (and continues to be required) to comply with, *inter alia*, the applicable industry standards requiring Target to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems—especially in its point-of-sale system—granting at least one outside vendor access to its internal computer network of systems through which the malware was placed inside Target's point-of-sale system, and failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' customers' sensitive payment card information and PII that was within Target's possession, custody and control. These standards include, without limitation, the PCI DSS, Visa Operating Regulations and MasterCard Rules—which establish the minimal duty of care owed by Target to Plaintiffs and Class Members.

129. By its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions, Target knowingly failed to comply with PCI DSS as evidenced, for example, by the theft and compromise of the payment card CVV codes and PIN numbers, which would not have been stolen had Target not stored the CVV codes and PIN numbers in its point-of-sale system in violation of PCI DSS. On information and belief, Target's point-of-sale system did not comply with PCI DSS in other ways that await discovery. Had Target been in PCI DSS compliance during the relevant time period, the Data Breach would not have occurred.

130. On information and belief, by its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions, Target also knowingly failed to comply with the Visa Operating Regulations and MasterCard Rules, the details of which await discovery and will most likely result in fines and other sanctions imposed by Visa and MasterCard.

131. Target's violations of the PCI DSS, Visa Operating Regulations and/or MasterCard Rules (and failure to implement the other above-described basic data security measures in its point-of-sale system and/or internal computer network) constitute negligence *per se* that directly and/or proximately caused Plaintiffs and Class Members to suffer the above-described substantial injuries. Plaintiffs and Class Members are members of the class of persons intended to be protected by the PCI DSS, Visa Operating Regulations, MasterCard Rules and other industry data security standards. The injuries suffered by Plaintiffs and Class Members—to wit, *inter alia*, expenses to cancel and reissue the compromised payment cards and/or absorption of unauthorized charges made on the compromised payment cards—were of the type intended to be prevented by these regulations and industry security standards.

COUNT VII

BREACH OF IMPLIED CONTRACT

132. The preceding factual statements and allegations are incorporated by reference.

133. Plaintiffs' and Class Members' customers were required to provide Target with their private, non-public, sensitive payment card information in order for Target to facilitate their payment card transactions. Implicit in this requirement was a covenant requiring Target to, *inter alia*, take reasonable efforts to safeguard and protect the payment card information and promptly notify Plaintiffs, Class Members, and their customers in the event their payment card information was stolen and compromised. Indeed, Target recognizes these obligations in its Privacy Policy on its website. This covenant also ran (and continues to run) to Plaintiffs and Class Members.

134. Similarly, by repeatedly and systematically requesting the authorization of millions of payment card transactions via the interstate and/or foreign wires, Target impliedly promised Plaintiffs and Class Members that its customer data security policies, procedures, protocols, and hardware and software systems—especially in its point-of-sale system—safeguarded and protected Plaintiffs' and Class Members' customers' private, non-public, sensitive payment card information and PII from unauthorized dissemination.

135. Notwithstanding the above-described implied contractual obligations, Target knowingly failed to safeguard and protect Plaintiffs' and Class Members' customers' private, non-public, sensitive payment card information. To the contrary, Target provided a gateway for the unauthorized dissemination of this information to fraudsters and other unauthorized third parties worldwide. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions breached its implied contracts with Plaintiffs and Class Members which, in turn, directly and/or proximately caused Plaintiffs and Class Members to suffer the above-described substantial financial injuries.

COUNT VIII

BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS ARE THIRD-PARTY BENEFICIARIES

136. The preceding factual statements and allegations are incorporated by reference.

137. At all relevant times, Target was (and, on information and belief, continues to be) in contractual relationships pertaining to its compromised point-of-sale system with (i) Bank of America Merchant Services, Target's acquiring bank for payment card transactions, (ii) Vantiv, Inc., Target's payment card transaction processor, and/or (iii) Target's network and point-of-sale system outside consultants and/or hardware and/or software vendors. Upon information and belief, Plaintiffs and Class Members are intended third-party beneficiaries of these contracts.

138. Upon information and belief, these contracts explicitly or implicitly require Target to implement customer data security policies, procedures, protocols, and hardware and software systems—especially in its point-of-sale system—to safeguard and protect Plaintiffs' and Class Members' customers' private, non-public, sensitive payment card information and PII from unauthorized dissemination.

139. Plaintiffs and Class Members are intended third-party beneficiaries of these contracts. Under the circumstances, recognition of a right to performance by Plaintiffs and Class Members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiffs and Class Members the benefit of the performance promised in the contracts.

140. By its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions, Target breached one or more of these contracts by, *inter alia*, failing to safeguard and protect Plaintiffs' and Class Members' customers' private, non-public, sensitive payment card information and PII that was stolen and compromised in the Target Data Breach,

which directly and/or proximately caused Plaintiffs and Class Members to suffer the above-described substantial damages. By its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions, Target saved (or avoided spending) a substantial sum of money by knowingly failing to comply with its contractual obligations the PCI DSS, the Visa Operating Regulations and the MasterCard Rules—and continues to do so.

COUNT IX

UNFAIR AND DECEPTIVE ACTS AND PRACTICES
UNDER MINN. STAT. § 325F.69, SUBD. 1

141. The preceding factual statements and allegations are incorporated by reference.

142. Target is headquartered in Minneapolis, Minnesota and, at all relevant times, was (and continues to be) engaged in trade or commerce in the State of Minnesota.

143. Plaintiffs and Class Members are financial institutions and other entities engaged in trade or commerce that issued payment cards stolen and compromised by the Data Breach.

144. On information and belief, the Target point-of–sale system and other systems within the Target internal computer network containing the stolen payment card information that were breached as part of the Data Breach are located in Minneapolis, Minnesota.

145. Target knew, and intentionally so acted, that Plaintiffs and Class Members are part of the Visa and MasterCard Networks and rely on merchants that accept Visa and MasterCard payment cards to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems—especially in its point-of-sale system. Target, however, intentionally devised, engaged in, condoned and/or ratified the above-described open-ended, unlawful and intentional schemes to (i) defraud and cheat Plaintiffs and Class Members to obtain money, funds, credits, assets, and/or other property owned by, or under the custody or control of, Plaintiffs and Class Members by means of false or fraudulent pretenses

and/or (ii) fraudulently and intentionally misrepresent to Plaintiffs and Class Members—explicitly and/or implicitly—through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate and/or foreign wires, its website, and its participation in the Visa Network and MasterCard Network that (a) it was in compliance with the Visa Operating Regulations and/or MasterCard Rules mandating the protection of payment card information and prohibiting the retention or storage of payment card account numbers, PIN numbers, personal information, magnetic stripe information, and/or transaction information subsequent to the approval of the transaction, (b) it was in compliance with the PCI DSS, and (c) its customer data security policies, procedures, protocols, and hardware and software systems were in place and would safeguard and protect sensitive customer data—including the stolen and compromised payment card information—for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Target and/or approve millions of payment card purchases made at Target via the interstate and/or foreign wires for the further purpose of increasing Target's revenue, profitability, and return on investment. Alternatively, Target fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse was true. By doing so, Target (i) directly and/or proximately caused Plaintiffs and Class Members to suffer damages to their businesses and/or property, (ii) saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (iii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members. Target intentionally engaged in these wrongful actions, inaction and/or omissions for its financial benefit and to Plaintiffs' and Class Members' financial detriment. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions constitute unfair and deceptive acts and practices within the meaning of Minn. Stat. § 325F.69, subd. 1.

146. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions also violated the Gramm-Leach-Bliley Act, 15 U.S.C. §6801, *et seq.*, and 16 C.F.R. §313, *et seq.*, which prohibit Target's misuse and/or inappropriate disclosure of the stolen payment card information. Target violated the Gramm-Leach-Bliley Act by improperly using and disclosing the stolen payment card information by, *inter alia*, (i) storing the stolen payment card information well beyond the permitted time frame, and/or (ii) failing to safeguard and protect the stolen payment card information in its point-of-sale system (and possibly other systems in its internal computer network, and/or (iii) allowing the payment card information to be stolen and compromised by others (the hackers) for purposes unrelated to processing payment card transactions. Such unlawful and intentional schemes, wrongful actions, inaction and/or omissions also constitute unfair and deceptive acts and practices within the meaning of Minn. Stat. § 325F.69, subd. 1.

147. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions leading to the theft and compromise of the payment card information constitute knowing and/or willful unfair and deceptive acts and practices with a direct and substantial effect in Minnesota and throughout the United States that, in turn, directly and/or proximately caused Plaintiffs and Class Members to suffer the above-described substantial damages—for which Plaintiffs and Class Members are entitled to compensation.

COUNT X

VIOLATION OF MINN. STAT. § 325E.64

148. The preceding factual statements and allegations are incorporated by reference.

149. Under Minnesota law:

> 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.

Minn. Stat. § 325E.64, subd. 2. Minnesota law further 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. … The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

Minn. Stat. § 325E.64, subd. 3.

150. Target's above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions leading to the theft and compromise of the payment card information breached Minn. Stat. § 325E.64, subd. 2 and directly and/or proximately caused Plaintiffs and Class Members to suffer the above-described substantial damages—for which Plaintiffs and Class Members are entitled to compensation under Minn. Stat. § 325E.64, subd. 3.

COUNT XI

UNJUST ENRICHMENT/ASSUMPSIT

151. The preceding factual statements and allegations are incorporated by reference.

152. Plaintiffs plead this Count in the alternative to its breach of contract claims (Counts VII and VIII) because Plaintiffs and Class Members cannot recover under this Count and under Count VII and/or Count VIII.

153. Target (and possibly others, the identities of whom are known only to Target at this time) have been (and continue to be) unjustly enriched by, *inter alia*, (i) the revenue from payment card transactions made on the stolen and compromised payment cards during the time of the Target Data Breach, (ii) the saved cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems in its point-of-sale system, (iii) the shifted the risk and expense of the Data Breach to Plaintiffs and Class Members, (iv) using and/or investing the fraudulently obtained revenue and profits from the payment card transactions described in (i) to participate in, create and/or operate various enterprises including, *inter alia*, the Visa Network, MasterCard Network, Target.com, Financial and Retail Services, Target Sourcing Services, Target Commercial Interiors, and/or Target Brands, and (v) the return on investment on the amounts described in (i)-(iv) (above).

154. Target, therefore, should be compelled to refund (or disgorge) such wrongfully collected and/or saved back funds under the common law equitable doctrine of unjust enrichment and/or the duty to make restitution under the common law equitable doctrine of assumpsit.

RELIEF REQUESTED

155. The preceding factual statements and allegations are incorporated by reference.

156. **ACTUAL, CONSEQUENTIAL, AND/OR INCIDENTAL DAMAGES.** As a direct and/or proximate result of the above-described unlawful and intentional schemes, wrongful actions,

inaction and/or omissions engaged in by Target (and/or its co-conspirators), Plaintiffs and Class Members have sustained (and will continue to sustain) actual, consequential, incidental, and/or statutory damages in the form of, *inter alia*, expenses to cancel and reissue compromised payment cards, expenses to notify payment cardholders affected by the Target Data Breach, the absorption of fraudulent charges made on the compromised payment cards, business destruction, lost profits and/or lost business opportunities—for which Plaintiffs and Class Members are entitled to compensation. Alternatively, Plaintiffs and Class Members are entitled to restitution and/or disgorgement of Target's gross revenue from payment card transactions made on the stolen and compromised payment cards generated during the time of the Target Data Breach and all other amounts by which Target (and its co-conspirators) have been unjustly enriched. All of the damages sustained by Plaintiffs and Class Members were reasonably foreseeable by Target. All conditions precedent to Plaintiffs' and Class Members' claims for relief have been performed and/or occurred.

157. **PUNITIVE DAMAGES.** The above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions engaged in by Target (and/or its co-conspirators) were committed intentionally, willfully, wantonly and/or with reckless disregard for Plaintiffs' and Class Members' rights and interests. Accordingly, Plaintiffs and Class Members are entitled to punitive damages from Target (and/or its co-conspirators) as punishment and to discourage such wrongful conduct in the future. All conditions precedent to Plaintiffs' and Class Members' claims for relief have been performed or occurred.

158. **RICO TREBLE DAMAGES.** Plaintiffs and Class Members also are entitled to automatic treble damages for the above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions engaged in by Target (and/or its co-conspirators) in violation of the RICO statute under 18 U.S.C. § 1964(c).

159. **INJUNCTIVE RELIEF.** The above-described repetitious and systematic interstate and/or foreign wire fraud in violation of 18 U.S.C. § 1343 engaged in by Target (and/or its co-conspirators) has caused (and will continue to cause) Plaintiffs and Class Members to suffer irreparable harm in the form of, *inter alia*, expenses to cancel and reissue compromised payment cards, the absorption of fraudulent charges made on the compromised payment cards, business destruction, lost profits and/or lost business opportunities. Such irreparable harm will not cease unless and until enjoined by this Court. Plaintiffs and Class Members, therefore, are entitled to a temporary injunction, permanent injunction and/or other appropriate affirmative relief including, *inter alia*, (i) restitution and/or disgorgement of Target's gross revenue from payment card transactions made on the stolen and compromised payment cards during the time of the Target Data Breach and all other amounts by which Target (and/or its co-conspirators) have been unjustly enriched, (ii) an order compelling Target to implement the proper customer data protection policies, procedures, protocols, hardware and/or software systems, and/or (iii) an order compelling Target (and/or its co-conspirators) to discontinue its above-described unlawful and intentional schemes, wrongful actions, inaction and/or omissions. All conditions precedent to Plaintiffs' and Class Members' claims for relief have been performed and/or occurred.

160. **ATTORNEYS' FEES, LITIGATION EXPENSES AND COURT COSTS.** Plaintiffs and Class Members also are entitled to recover their attorneys' fees, litigation expenses, and court costs under, *inter alia*, 18 U.S.C. § 1964(c). All conditions precedent to Plaintiffs' and Class Members' claims for attorneys' fees, litigation expenses and court costs have been performed and/or occurred.

PRAYER

WHERFORE, Plaintiffs, for themselves and Class Members, respectfully request that (i) Target be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii)

Plaintiffs be designated the Class Representatives, and (iv) Plaintiffs' counsel be appointed as Class Counsel. Plaintiffs, for themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against Target in favor of Plaintiffs and Class Members, for:

(a) With respect to Counts I–III (violations of 18 U.S.C. § 1961, *et seq.*)--

(i) threefold the actual, consequential and/or incidental damages sustained by Plaintiffs and Class Members, along with attorneys' fees, litigation expenses, and court costs, all pursuant to 18 U.S.C. § 1964(c), together with pre- and post-judgment interest at the highest legal rates;

(ii) equitable relief, as may be appropriate, pursuant to 18 U.S.C. § 1964(a), including an equitable accounting for all benefits, consideration, and gross revenue received, directly or indirectly, by Target (and/or its co-conspirators) from payment card transactions made on the stolen and compromised payment cards during the time of the Target Data Breach, including the imposition of a constructive trust, the voiding of unlawful transfers, the disgorgement of all ill-gotten gross revenue, and/or all amounts by which Target (and/or its co-conspirators) have been unjustly enriched; and

(iii) injunctive relief (as set forth above).

(b) With respect to Counts IV–XI:

(i) actual, consequential, incidental, and/or statutory damages to be determined by the trier of fact;

(ii) punitive damages;

(iii) all amounts by which Target (and/or its co-conspirators) have been unjustly enriched;

(iv) an equitable accounting for all benefits, consideration, and gross revenue received, directly or indirectly, by Target (and/or its co-conspirators) from payment card transactions made on the stolen and compromised payment cards during the time of the Target Data Breach, including the imposition of a constructive trust, the voiding of unlawful transfers, the disgorgement of all ill-gotten gross revenue, and/or all amounts by which Target (and/or its co-conspirators) have been unjustly enriched;

(v) injunctive relief (as set forth above);

(vi) pre- and post-judgment interest at the highest legal rates;

(vii) attorneys' fees, litigation expenses and costs of suit incurred through the trial and any appeals of this case; and

(c) For all Counts, such other and further relief the Court deems just and proper.

JURY DEMAND

Plaintiffs, for themselves and all others similarly situated, respectfully demand a trial by jury on all claims so triable.

Date: February 13, 2014.

Respectfully submitted,

By: /s/ *Richard L. Coffman*

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

Mitchell A. Toups
WELLER, GREEN TOUPS & TERRELL, LLP
2615 Calder Ave., Suite 400
Beaumont, TX 77702
Telephone: (409) 838-0101
Facsimile: (409) 838-6780 (FAX)
Email: matoups@wgttlaw.com

G. Robert Blakey
Professor of Law Emeritus
Notre Dame Law School*
7002 East San Miguel Ave.
Paradise Valley, AZ 85253
Telephone: (574) 514-8220
Email: blakey.1@nd.edu
* Noted for identification only

ATTORNEYS FOR PLAINTIFFS AND THE PUTATIVE CLASS