UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF KENTUCKY
LOUISVILLE DIVISION
CASE NO. 3:14-cv-35-H

Tricia Meeley on behalf of herself and a Class of persons similarly situated,	)	
PLAINTIFF	)	**JURY TRIAL DEMANDED**
v.	)	
TARGET CORPORATION	)	
DEFENDANT	)	

* * * * * * * *

CLASS ACTION COMPLAINT

Plaintiff Tricia Meeley ("Plaintiff" or "Plaintiff MEELEY"), individually and on behalf of all other persons similarly situated, brings this Class Action Complaint against TARGET CORPORATION ("Defendant" or "Defendant TARGET"). The Plaintiff makes the following allegations, except as to allegations specifically pertaining to the Plaintiff and the Plaintiff's counsel, based upon information and belief and based upon, *inter alia*, the investigation of the Plaintiff's counsel and the review of public documents including the Defendant's press release and various news articles.

NATURE OF THIS ACTION

1. The Plaintiff brings this class action suit on her own behalf and on behalf of all other persons or entities in the United States against the Defendant to redress the Defendant's failure to adequately safeguard certain credit card and debit card information and related data,

arising from the Defendant's failure to adequately secure customer credit and debit card data. As a result of the Defendant's wrongful actions, customer information was stolen from the Defendant's computer network that handles a wide range of financial information for millions of customers, including credit cards, debit cards linked to checking accounts, and transactions for returned merchandise. As a result of the Defendant's actions or inactions, millions of its customers have had their personal financial information compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identity theft, and have otherwise suffered damages.

JURISDICTION AND VENUE

2. Jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1332(d), as the matter in controversy exceeds $5 million, diversity of citizenship exists between the Plaintiff and the Defendant, and there are believed to be more than 100 class members.

3. Venue properly lies in this District pursuant to 28 U.S.C. § 1391(a)(2), since the cause of action arose in this District, and the unlawful conduct of Defendant, out of which the cause of action arose, took place in this District.

PARTIES

4. The Plaintiff, Tricia Meeley, resides in Louisville, Kentucky. The Plaintiff had her personal and financial information stolen via her credit card data information from the Defendant's computer system, and has been damaged as a result.

5. The Defendant, Target Corporation, is a Minnesota corporation with its headquarters at 1000 Nicollet Mall Minneapolis, Minnesota. Target operates retail chains in Kentucky and throughout the United States

FACTS

6. The Defendant operates a chain of approximately 1,797 retail stores and 37 distribution centers across 49 states and the District of Columbia. The company had revenues of approximately $69.87 Billion in 2012, and has stock that is traded on the New York Stock Exchange under the ticker symbol TGT.

7. On December 18, 2013, the blog *KrebsOnSecurity* reported that the Defendant was investigating a security breach of potentially millions of its customers' credit and debit card information between November 29, 2013 and December 15, 2013.[1] According to the report, the breach involved the theft of data stored on the magnetic stripe on the credit and debit cards. This theft of this data, known as "track data," allows thieves to produce counterfeit cards by encoding the information from the stolen data onto any card with a magnetic stripe, and includes the card number, cardholder name, the card's expiration date, and the card's CVV number.

8. On December 20, 2013, the Defendant first publicly announced that it had been hit by a wide- reaching security breach that had the potential leave millions of its customers around the world exposed to fraud and identity theft. The transactions at issue could date back several months. The Defendant's press release stated, in relevant part:

> Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issues. …
>
> Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions

[1]Brian Krebs, *Sources: Target Investigating Data Breach,* Krebs on Security (accessed January 14, 2014), http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

> immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts.

9. *KrebsOnSecurity* reported on December 20, 2013 that the stolen data was being sold on the black market in batches of one million cards at prices ranging from approximately $20 to $100 per card. The report further noted that the breach had been independently confirmed by a fraud analyst at a major bank after the analyst was able to purchase the information of many of the bank's cards from an online store dealing in the illegal trade of stolen credit and debit cards.[2]

10. On December 27, 2013, Target disclosed that encrypted PIN data for the stolen debit cards had also be compromised during the breach.

11. On January 10, 2014, Target disclosed that the data breach had also exposed the names, mailing addresses, phone numbers and email addresses for up to 70 million individuals.

12. It is now believed that the information may have been obtained through the use of a form a malware installed on point-of-sale systems known as RAM scrapers, which steal payment card data before it can be encrypted by a point-of-sale system. In 2013, Visa issued two warnings addressing the threat posed by RAM scrapers and memory parsing malware. [3]

13. The four major credit card companies, Visa, MasterCard, Discover, and American Express, jointly created the Payment Card Industry Data Security Standard (PCI DSS) in 2004,

---

[2] Brian Krebs, *Cards Stolen in Target Breach Flood Underground Markets,* Krebs on Security (accessed January 14, 2014), http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

[3] *Preventing Memory Parsing Malware on Grocery Merchants*, issued April 11, 2013, http://usa.visa.com/download/merchants/alert-prevent-grocer-malware-attacks-04112013.pdf; *Retail Merchants Targeted by Memory-Parsing Malware - UPDATE*, issued August 2013,http://usa.visa.com/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf

and the most recent revision, known as PCI 2.0, was adopted in 2010. Requirements to be PCI compliant include a secure network employing the use of firewalls the network, the use of secure repositories to protect cardholder information and the use of digital encryption, the use of anti-virus and anti-malware solutions to protect against malicious activity, restrictions on access to system information and operations, the monitoring of networks to ensure all safety measures are in place and functioning properly, and the maintenance of a formal information security policy. At this time, it is not known if Target was PCI compliant when the breach occurred.

14. Industry experts have commented that it is unlikely that Target was PCI compliant at the time of the breach, due to the length of time the breach went unnoticed.[14]

15. As a result of this breach of security, Class members' debit cards and credit cards were exposed; Plaintiffs and Class members were required to expend time, energy and expense to address and resolve these financial disruptions and mitigate the consequences by purchasing credit reports; credit monitoring and/or identity theft protection; they have suffered consequential emotional distress; mental anguish; and their credit and debit card information is at an increased risk of theft and unauthorized use.

16. According to media reports, fraudulent purchases using credit and debit card numbers stolen from Target have already surfaced in various states.

17. The security breach at Target is currently being investigated by the U.S. Secret Service and other law enforcement agencies.

---

[14]Byron Achohido, *Q&A: PCI rules could help stymie Target data thieves*, USA Today (accessed January 14, 2014), http://www.usatoday.com/story/cybertruth/2013/12/23/qa-pci-rules-could-help-stymie-target-data-thieves/4179941/

18. Upon information and belief, during the Class Period, the Defendant failed to adequately safeguard and protect the private and confidential debit card and credit card information of the Plaintiff and Class members, so that wrongdoers were able to obtain access to such data within the Defendant's information technology systems or in the course of transmission of the data to financial institutions.

19. Upon information and belief, lack of adequate security in the Defendant's information technology systems enabled the wrongdoers to install software used on point-of-sales terminals used to swipe magnetic strips on payment cards.

20. Upon information and belief, the Defendant did not adequately monitor their information technology system for the presence of foreign software in a manner that would enable them to detect this intrusion, so that the breach of security and diversion of customer information was able to continue unnoticed for over two weeks, or longer, during the height of the 2013 Holiday shopping season. This was an act which harmed the Plaintiff and Class members by increasing the risk of future harm that the Plaintiff and Class members would have otherwise faced, absent the Defendant's actions. Upon information and belief, the Defendant did not abide by best practices and industry standards concerning the security of its computer systems, payment processing systems and or information technology systems.

21. The Plaintiff shopped at Target in Louisville, Kentucky, multiple times in December 2013 using both her credit and debit cards for payment. The Plaintiff, as well as others in the proposed class, has been instructed by the Defendant to "periodically obtain credit reports from each nationwide credit reporting agency" to ascertain and/or discover whether they have experienced fraudulent transactions arising from the Defendant's wrongful conduct.

Consequently, the Plaintiff and others have been damaged and continue to suffer damages as a result of The Defendant's wrongful conduct.

CLASS ACTION ALLEGATIONS

22. The Plaintiff brings this class action, pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), on behalf of herself and all others similarly situated, consisting of all persons or entities in the State of Kentucky who have had personal or financial data stolen from the Defendant's computer network, and who were damaged thereby (the "Class"). The Class does not include the Defendant, nor its officers, directors, agents, or employees.

23. The Plaintiff brings this class action, pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), on behalf of herself and all others similarly situated, consisting of all persons or entities in the United States who have had personal or financial data stolen from the Defendant's computer network, and who were damaged thereby (the "Class"). The Class does not include the Defendant, nor its officers, directors, agents, or employees.

24. The Class consists of possibly millions of customers of Target located throughout Kentucky and the United States. While the exact number of Class members and the identities of individual Class members are unknown at this time, and can only be ascertained through appropriate discovery, based on the fact that hundreds of thousands of customer accounts have already been affected, the Class is so numerous that joinder of all Class members is impracticable.

25. The Defendant's conduct affected all Class members in exactly the same way. The Defendant's failure to properly safeguard its customers' personal and financial data and in failing to notify customers of the security breach as soon as practical after the breach was discovered is completely uniform among the Class.

26. Questions of law and fact common to all Class members predominate over any questions affecting only individual members. Such questions of law and fact common to the Class include:

a. whether the Defendant acted wrongfully by failing to properly safeguard its customers' financial data;

b. whether the Defendant failed to notify Class members of the security breach as soon as practical after the breach was discovered;

c. whether the Plaintiff and the Class have been damaged, and, if so, what is the appropriate relief as to each member of the Class; and

d. whether the Defendant breached implied contracts with Class members by failing to properly safeguard their private and confidential financial and personal data.

27. The Plaintiff's claims, as described herein, are typical of the claims of all Class members, as the claims of the Plaintiff and all Class members arise from the same set of facts regarding the Defendant's failure to protect Class members' financial data. The Plaintiff maintains no interests that are antagonistic to the interests of other Class members.

28. The Plaintiff is committed to the vigorous prosecution of this action and has retained competent counsel experienced in the prosecution of class actions of this type. Accordingly, the Plaintiff is an adequate representatives of the Class and will fairly and adequately protect the interests of the Class.

29. This class action is a fair and efficient method of adjudicating the claim of the Plaintiff and the Class for the following reasons:

a. common questions of law and fact predominate over any question affecting any individual Class member;

b. the prosecution of separate actions by individual members of the Class would likely create a risk of inconsistent or varying adjudications with respect to individual members of the Class thereby establishing incompatible standards of conduct for Defendant or would allow some Class members' claims to adversely affect other Class members' ability to protect their interests;

c. this forum is appropriate for litigation of this action since the cause of action arose in this District;

d. The Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

e. the Class is readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

30. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

COUNT I
NEGLIGENCE

31. The Plaintiff adopts and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

32. The Defendant assumed a duty to use reasonable care to keep the credit card and other nonpublic information of the Class that is, or was, in its possession and control private and secure. By its acts and omissions described herein, the Defendant unlawfully breached this duty. The Class was damaged by the Defendant's breach of this duty.

33. The private financial information of the Class that was compromised by the breach of the Defendant's security included, without limitation, information that was being improperly

stored and inadequately safeguarded in violation of, among other things, industry rules and regulations. The adoption of the rules and regulations contained in PCI 2.0 created a duty of reasonable care and standard of care that, upon information and belief, was breached by the Defendant.

34. The breach of security was a direct and proximate result of the Defendant's failure to use reasonable care to implement and maintain appropriate security procedures reasonably designed to protect the credit and debit card information and other nonpublic information of the Class. This breach of security and unauthorized access to the private, nonpublic information of the Class was reasonably foreseeable, particularly in light of the warnings regarding RAM scrapers issued by Visa in 2013.

35. The Defendant was in a special fiduciary relationship with the Class by reason of its entrustment with credit and debit card information and other nonpublic information. By reason of this fiduciary relationship, the Defendant had a duty of care to use reasonable means to keep the credit and debit card information and other nonpublic information of the Class private and secure. The Defendant also had a duty to inform Class members in a timely manner when their credit and debit card information and other nonpublic information became compromised. The Defendant has unlawfully breached these duties.

36. Pursuant to the Class members' rights to privacy, the Defendant had a duty to use reasonable care to prevent the unauthorized access, use, or dissemination of the credit and debit card information and other nonpublic information. The Defendant unlawfully breached this duty.

37. The compromise of the Class' nonpublic information, and the resulting burden, fear, anxiety, emotional distress, loss of time spent seeking to prevent or undo any further harm, and

other economic and non-economic damages to the Class, were the direct and proximate result of Defendant's violation of its duty of care.

38. The Defendant had a duty to timely disclose the data compromise to all customers whose credit and debit card information and other nonpublic information was, or was reasonably believed to have been, accessed by unauthorized persons. Disclosure was required so that, among other things, the affected customers could take appropriate measures to avoid unauthorized charges on their accounts, cancel or change account numbers on the compromised cards, and monitor their account information and credit reports for fraudulent charges. The Defendant breached this duty by failing to notify Class members in a timely manner that their information was compromised. The Class members were harmed by the Defendant's delay because, among other things, fraudulent charges have been made to the Class members' accounts.

39. The Defendant knew or should have known that its network for processing and storing credit and debit card transactions and related information had security vulnerabilities. The Defendant was negligent in continuing such data processing in light of those vulnerabilities and the sensitivity of the data.

40. As a direct and proximate result of the Defendant's conduct, the Class suffered damages including, but not limited to, loss of control of their credit card and other personal financial information; monetary loss for fraudulent and/or unauthorized charges incurred on their accounts; fear and apprehension of fraud, loss of money, and identity theft; the burden and cost of closing compromised accounts and opening new accounts; the burden of closely scrutinizing credit card statements for past and future transactions; damage to their credit history; loss of privacy; and other economic damages.

COUNT II
BREACH OF IMPLIED CONTRACT

41. The Plaintiff adopts and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

42. The Plaintiff and Class members would not have entrusted their private and confidential financial and personal information to the Defendant in the absence of such an implied contract with Defendant.

43. The Defendant breached the implied contracts it had made with the Plaintiff and Class members by failing to safeguard such information.

44. The damages sustained by the Plaintiff and Class members as described above were the direct and proximate result of the Defendant's breaches of these implied contracts.

COUNT IV
VIOLATION OF THE KENTUCKY
CONSUMER PROTECTION ACT
KRS 367.110 et seq.

45. Plaintiff, individually and on behalf of all others similarly situated, repeats, realleges, and incorporates by reference each of the foregoing and subsequent allegations of this Complaint as if fully set forth herein.

46. Under the Kentucky Consumer Protection Act, KRS 367.110, *et seq.*, (hereinafter referred to as "KCPA"), Defendant's practices as described above constitute "trade or commerce" within the meaning of KRS 367.170.

47. Plaintiff and the Class expected, and Defendant assured, that Plaintiff's personal information and non-public information maintained by Defendant would be protected and that it would not be disclosed to third parties.

48. KCPA prohibits unfair, false, misleading, unconscionable or deceptive acts.

49. Under KCPA, Defendant had a statutory duty to refrain from engaging in deceptive trade practices in connection with knowingly permitting the personal information to be exposed through an unsecure network that was not PCI compliant.

50. Under KCPA, Defendant had a statutory duty to refrain from engaging in deceptive trade practices.

51. Defendant's practice and course of conduct as alleged above is likely to mislead – and has misled – the consumer acting reasonably under the circumstances and has harmed consumers as a result.

52. Defendant's conduct violated the statutory duties described above.

53. Each of the aforementioned actions and failures to act of Defendant constitute unfair or unconscionable acts or practices in the conduct of trade or commerce, in violation of the KCPA.

54. As a result of said deceptive trade practices, Defendant has directly, foreseeably, and proximately caused damages to Plaintiff and the proposed Class. Defendants' policies and practices as alleged herein constitute unfair trade practices under KCPA, as they offend the public policy of the State of Kentucky and the United States, are unethical, oppressive, and unscrupulous, and cause substantial injury to Kentucky consumers, including the Plaintiff and proposed Class.

55. Defendant's practices as alleged are immoral, unethical, oppressive, or unscrupulous and cause substantial injury to consumers.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

a. that this Court certify this action as a Class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and appoint the Plaintiff and her counsel to represent the Class;

b. that this Court enter judgment in favor of the Plaintiff and the Class, and against the Defendant under the legal theories alleged herein;

c. that this Court award damages under the common law theories alleged herein;

d. that this Court award attorneys' fees, expenses, and costs of this suit;

e. that this Court award the Plaintiff and the Class pre-judgment and post-judgment interest at the maximum rate allowable by law; and

f. that this Court award such other and further relief as it may deem just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of all others similarly situated, demands a trial by jury on all issues so triable.

Dated: January 15, 2014

Respectfully submitted,

JONES WARD PLC
Jasper D. Ward
Alex C. Davis

/s/ Jasper D. Ward
Marion E. Taylor Building
312 S. Fourth Street, 6th Floor
Louisville, Kentucky 40202
Telephone: (502) 882-6000
jasper@jonesward.com
alex@jonesward.com

Attorneys for Plaintiff and the Proposed Class