IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF ALABMA
NORTHERN DIVISION

ALABAMA STATE EMPLOYEES CREDIT UNION,	)	
Plaintiff,	)	Civil Action No: 2:13-cv-952- WHA-CSC
-vs-	)	
TARGET CORPORATION,	)	JURY TRIAL DEMANDED
Defendant.	)	

PLAINTIFF'S FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Alabama State Employees Credit Union ("Plaintiff" or "ASE Credit Union") hereby brings this class action suit against Target Corporation ("Target" or "Defendant"). Plaintiff makes the following allegations, except as to allegations specifically pertaining to Plaintiff and Plaintiff's counsel, based upon the investigation undertaken by Plaintiff's counsel, which included, *inter alia*, Plaintiff's personal knowledge, review and analysis of Defendant's website, press release, and various news articles.

NATURE OF THIS ACTION

1. Plaintiff brings this class action suit on its own behalf and on behalf of all other financial institutions or entities in the United States against Target to redress TARGET's failure to adequately safeguard certain credit card and debit card information and related data of Plaintiff's and Class Members' customers and members. More specifically, this action arises from TARGET's failure to maintain adequate computer data security of customer credit and

debit card data, which was accessed and stolen by computer hackers. As a result of TARGET's wrongful actions, customer information was stolen from TARGET'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. Because of TARGET's actions, 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. Plaintiff and Class Members have been defrauded of the deposits of their customers and members, resulting in financial losses to Plaintiff and Class Members in refunding those losses and the cost of closing accounts and reissuing new checks, debit cards, and credit cards to customers and members as a result of TARGET's data breach.

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, Plaintiff has diverse citizenship from Defendant TARGET, and there are 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. Plaintiff ASE Credit Union is an Alabama corporation with its headquarters in Montgomery, Alabama. Plaintiff's customers and members had their personal and financial information stolen via their debit and credit card data information from TARGET's computer system(s), and has been damaged as a result of refunding the losses to Plaintiff's customers and

members and due to the cost of closing accounts and reissuing new checks, debit cards, and credit cards to customers and members as a result of TARGET's data breach.

5. Defendant TARGET is a Minnesota corporation with its headquarters at 1000 Nicollet Mall Minneapolis, MN. TARGET operates retail chains in Alabama and throughout the United States.

OPERATIVE FACTS

6. TARGET purports to be the leading off-price apparel and home fashion retailer in the United States and worldwide, with $69.87 billion in revenues in 2012. Its stock trades on the New York Stock Exchange under the symbol TGT. TARGET operates more than 1,797 retail stores. These stores are located across the United States.

7. On December 20, 2013, TARGET first publicly announced that it had been hit by a wide- reaching security breach that may leave millions of its customers around the world exposed to fraud and identity theft. The transactions at issue could date back several months. TARGET'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 immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts.

8. U.S. retailers, including TARGET, are required to follow stringent card-industry rules. The rules that cover transactions on cards branded with logos from Visa, MasterCard International Inc., American Express Co. and Discover Financial Services, require merchants to validate a series of security measures, such as the establishment of firewalls to protect databases. Among other things, merchants are prohibited from storing

unprotected cardholder information.

9. The stolen data includes among other things, customer names, credit and debit card numbers, card expiration dates and the three-digit security codes located on the backs of cards. There is no legitimate reason for TARGET to keep all of this information stored electronically.

10. As a result of TARGET's breach of its security, the Class Members' customers and members' debit cards and credit cards were exposed; Plaintiff and Class Members were required to expend time, energy and expense to address and resolve these financial disruptions and mitigate the consequences by refunding loss deposits; issuing new credit and debit cards; closing compromised or suspected-to-be compromised accounts; opening new accounts; and increased costs in monitoring customer and member accounts to determine which transactions are legitimate or fraudulent.

11. According to media reports, fraudulent purchases using credit and debit card numbers stolen from TARGET have already surfaced in various states, including Alabama.

12. One TARGET customer said that she found two unauthorized charges on her card that she fears were related to the breach.

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

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

15. Lack of adequate security in 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.

16. 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 Plaintiff and Class Members by increasing the risk of future harm that Plaintiff and Class Members would have otherwise faced, absent the Defendant's actions. TARGET did not abide by best practices and industry standards concerning the security of its computer systems, payment processing systems and or information technology systems.

17. Plaintiff has been swamped by customers and its members needing to close accounts due to TARGET's data breach, resulting in Plaintiff exerting time, resources, and money to close out accounts and open new accounts with different account numbers. Each opening of a new account results in losses to the Plaintiff due to the costs associated with printing new checks, creating new debit and credit cards, etc. during the height of the 2013 Holiday season, when retail sales are at their highest.

18. Plaintiff has lost significantly in refunding the unauthorized use and access of its customers and members accounts due to TARGET's data breach. The cost in refunding loss deposits, time, and resources spent to remedy the situation of Plaintiff's customers and members are untold.

CLASS ACTION ALLEGATIONS

19. Plaintiff brings this class action, pursuant to Federal Rule of Civil Procedure 23(a)

and (b)(3), on behalf of itself and all others similarly situated, consisting of all financial institutions and entities (including, but not limited to, banks and credit unions) in the State of Alabama that have had the personal or financial data of their customers and members stolen from TARGET's computer network, and who were damaged thereby (the "Class"). The Class does not include TARGET, or its officers, directors, agents, or employees.

20. Plaintiff brings this class action, pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), on behalf of itself and all others similarly situated, consisting of all financial institutions and entities (including, but not limited to, banks and credit unions) in the United States who have had personal or financial data stolen from TARGET's computer network, and who were damaged thereby (the "Class"). The Class does not include TARGET, or its officers, directors, agents, or employees.

21. The Class consists of possibly thousands of financial institutions and entities of TARGET's customers located throughout Alabama 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.

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

23. 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 Defendant acted wrongfully by failing to properly safeguard Class Members' customers' financial data (including, but not limited to, the account numbers and credit and debit card numbers assigned by Class Members to protect customers' deposits and credit);

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

c. whether 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 Defendant breached implied contracts with Class Members by failing to properly safeguard their customers' private and confidential financial and personal data.

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

24. 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, Plaintiff is an adequate representative of the Class and will fairly and adequately protect the interests of the Class.

25. This class action is a fair and efficient method of adjudicating the claim of 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. Plaintiff is not aware of any other litigation of these issues ongoing in this State or elsewhere brought by a nationwide class of consumers of TARGET;

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

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

f. 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.

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

COUNT I
NEGLIGENCE

28. Plaintiff repeats and re-alleges the allegations contained in the foregoing

paragraphs as if fully set forth herein.

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

30. The private financial information of the Class that was compromised by the breach of 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. According to The Wall Street Journal on January 19, 2007, "[p]eople familiar with the situation have said that TARGET doesn't comply with those [industry] requirements." Those rules and regulations created a duty of reasonable care and a standard of care that was breached by Defendant.

31. The breach of security was a direct and proximate result of 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's customers. This breach of security and unauthorized access to the private nonpublic information of the Class's customers was reasonably foreseeable.

32. Defendant was in a special fiduciary relationship with the Class by reason of its entrustment with checking account, savings account, money market account, credit and debit card information and other nonpublic information. By reason of this fiduciary relationship, Defendant had a duty of care to use reasonable means to keep the checking account, savings account, money market account, credit and debit card information and other nonpublic information of the Class's customers private and secure. Defendant also had a duty to inform

Class Members in a timely manner when their customers and members' checking account, savings account, money market account, credit and debit card information and other nonpublic information became compromised. Defendant has unlawfully breached these duties.

33. Pursuant to Class Members' customers' rights to privacy, Defendant had a duty to use reasonable care to prevent the unauthorized access, use, or dissemination of the checking account, savings account, money market account, credit and debit card information and other nonpublic information. Defendant unlawfully breached this duty.

34. The compromise of the Class's nonpublic information, and the resulting burden, resources, cost, 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.

35. Defendant had a duty to timely disclose the data compromise to all Class Members whose customers' checking account, savings account, money market account, 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 Class Members could take appropriate measures to avoid unauthorized charges on customers' accounts; assist in the speedy cancellation or changing of account numbers on the compromised cards; and monitoring of Class Members' customer account information for fraudulent charges. Defendant breached this duty by failing to notify Class Members in a timely manner that their information was compromised. Class Members were harmed by Defendant's delay because, among other things, fraudulent charges have been made to Class Members' customer accounts, resulting in damages to Class Members.

36. Defendant had a duty to use reasonable care to destroy, and not unnecessarily

store, checking account, savings account, money market account, credit and debit card information and other personal information of the Class Members' customers. By the acts described herein, Defendant negligently breached this duty, and the Class was harmed thereby.

37. Defendant knew or should have known that its network for processing and storing checking account, savings account, money market account, credit and debit card transactions and related information had security vulnerabilities. Defendant was negligent in continuing such data processing in light of those vulnerabilities and the sensitivity of the data.

38. As a direct and proximate result of Defendant's conduct, the Class suffered damages including, but not limited to, loss of control of the checking account, savings account, money market account, credit and debit card and other personal financial information they charged with protecting on behalf of their customers and members; monetary loss for reimbursing fraudulent and/or unauthorized charges incurred on their customers' accounts; the burden and cost of monitoring accounts to verify legitimate from fraudulent charges on their customers and members accounts; the burden and cost of closing compromised accounts and opening new accounts for their customers and members; and other economic damages.

COUNT II
BREACH OF IMPLIED CONTRACT

39. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

41. Defendant breached the implied contracts it had made with Plaintiff and Class Members by failing to safeguard such information.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of itself and all others similarly situated, respectfully request 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 Plaintiff and its counsel to represent the Class;

b. that this Court enter judgment in favor of Plaintiff and the Class, and against Defendant TARGET 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 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.

JURY TRIAL DEMAND

Plaintiff, on behalf of itself and the Class, demands a trial by jury on all issues so triable.

Respectfully submitted,

/s/ Larry A. Golston, Jr.
JERE L. BEASLEY (BEA020)
W. DANIEL "DEE" MILES, III (MIL060)
LARRY A. GOLSTON (GOL029)
ANDREW E. BRASHIER (BRA156)
Attorneys for Plaintiffs

OF COUNSEL:

BEASLEY, ALLEN, CROW, METHVIN,
PORTIS & MILES, P.C.
272 Commerce Street
Post Office Box 4160
Montgomery, Alabama 36103-4160
(334) 269-2343
(334) 954-7555 FAX

CERTIFICATE OF SERVICE

I hereby certify that on the 2nd day of January, 2014, I have served a copy of the foregoing upon all counsel listed below by e-file and/or by placing a copy of the same in the United States Mail, postage prepaid to the following:

Target Corporation
Registered Agent: CT Corporation System
2 North Jackson Street
Montgomery, Alabama 36104

/s/ Larry A. Golston, Jr.
OF COUNSEL