IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

FIRST CHOICE FEDERAL CREDIT UNION, individually and on behalf of a class of all similarly situated financial institutions, Plaintiff, v. TARGET CORPORATION, Defendant.	Case No: CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiff First Choice Federal Credit Union, through its undersigned counsel, individually and on behalf of all similarly situated financial institutions, files this Class Action Complaint against Defendant Target Corporation ("Target" or "Defendant").

NATURE OF THE ACTION

1. This is a class action on behalf of credit unions who suffered injury as a result of a security breach compromising Target store customers' names, credit and debit card numbers, card expiration dates, personal identification numbers ("PINs"), and card verification values ("CVVs") (hereinafter the "Target Data Breach"), forcing these institutions to (a) cancel or reissue any access device affected by the Target Data Breach; (b) close any deposit, transaction, share draft, or other accounts affected by the breach, including but not limited to stopping payments or blocking transactions with respect to the accounts; (c) open or reopen any deposit, transaction, share draft, or other accounts affected by the Target Data Breach; (d) refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Target Data Breach; or (e) notify cardholders affected by the Target Data Breach.

2. As alleged herein, the injuries to Plaintiff and the Class were caused by Defendant's failure to maintain adequate computer data security of customer information, including credit and debit card data, as well as personally identifying information. Upon information and belief, Defendant also failed to remove or delete card security code data, the PIN verification code number, and/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, in express violation of Minn. Stat. Ann. § 325E.64 Subd. 2.

3. As a result of Defendant's wrongful actions, customer information was stolen from Target's computer network. Millions of Defendant's customers have had their personal financial information compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Additionally, Plaintiff and members of the Class have incurred and will continue to incur significant costs associated with, among other things, notifying its members of issues related to the Target Data Breach, closing out and opening new customer accounts, reissuing members' cards, and/or refunding members' losses resulting from the unauthorized use of their accounts.

4. Plaintiff, on behalf of the Class seeks to recover damages caused by Defendant's unfair and/or deceptive acts or practices in violation of Minn. Stat. Ann. § 325F.69 Subd. 1 (Count I); acts in violation of Minn. Stat. Ann. § 325E.64 (Count II), and negligence (Count III).

5. Plaintiff, on behalf of the Class also seeks a finding that Defendant improperly retained customer data and injunctive relief enjoining Defendant from such improper retention of information.

JURISDICTION AND VENUE

6. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class defined below, many of whom reside in different states than Defendant.

7. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because Plaintiff maintains its principal place of business in this District, Defendant regularly transacts business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

PARTIES

8. Plaintiff First Choice Federal Credit Union is a federally chartered credit union with its principal place of business located in New Castle, Pennsylvania.

9. Defendant Target Corporation is a Minnesota corporation with its principal place of business located in Minneapolis, Minnesota. Target operates a chain of retail stores that sell merchandise, including home goods, electronics, and clothing. Target owns over 1,790 stores in the United States.

FACTUAL BACKGROUND

The Target Data Breach Unravels

10. On December 18, 2013, respected security blogger, Brian Krebs reported that "Target is investigating a data breach potentially involving millions of customer credit and debit card records." *See* Krebs on Security December 18, 2013 Blog Post, *available at*

http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/[1] (attached hereto as Exhibit A).

11. Following Mr. Kreb's announcement, on December 19, 2013, Target issued a statement confirming that a security breach occurred and asserted that 40 million credit and debit card accounts may have been impacted between November 27, 2013 and December 15, 2013. *See* "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," *available at* http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores (hereinafter "December 19, 2013 Press Release") (attached hereto as Exhibit B).

12. Not until December 20, 2013, over three weeks after the data breach began, did Target reach out to its impacted customers to inform them of the issue. *See* December 20, 2013 Target Email to Customers, *available at* https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca (attached hereto as Exhibit C).

13. In the December 20, 2013 Target Email to Customers, Target admitted that the security breach "included customer name, credit or debit card number, and the card's expiration date and CVV." *See* Exhibit C.

14. Target further acknowledged that "encrypted debit card PIN data was among the information stolen when its systems were breached during the peak holiday shopping period." Target noted that "its investigation now shows that encrypted PIN data was 'removed' from its systems." *See* "Target Says Encrypted PIN Data Taken in Breach," THE WALL STREET JOURNAL, Dec. 27, 2013, *available at* http://online.wsj.com/news/articles/SB10001424052702303345104579284440022934198?cb=logged0.0365547111723572 (attached hereto as Exhibit D).

[1] All cited websites were last visited on January 22, 2014.

15. Then, on January 10, 2014, Target made another announcement, this time conceding that its "investigation has determined that the stolen information includes names, mailing addresses, phone numbers or email addresses for up to 70 million individuals." *See* "Target Provides Update on Data Breach and Financial Performance," *available at* http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance (hereinafter "January 10, 2014 Target Press Release") (attached hereto as Exhibit E).

16. Reports have shown that the information for the 70 million individuals was stored separately from the 40 million credit and debit card accounts that Target previously admitted was impacted. *See* "Target Now Says 70 Million People Hit in Data Breach," THE WALL STREET JOURNAL, Jan. 10, 2014, *available at* http://online.wsj.com/news/articles/SB10001424052702303754404579312232546392464 (attached hereto as Exhibit F).

17. In combination with the initially reported 40 million customers whose credit and debit card accounts were affected, the Target data breach impacted approximately up to 110 million consumers. *See* Exhibit F.

18. As a result of Target's wrongful conduct, sensitive customer information was accessed from Target's computer systems. Indeed, "[f]raud experts said the information stolen from Target's systems quickly flooded the black market. On Dec. 11, shortly after hackers first breached Target, Easy Solutions, a company that tracks fraud, noticed a 10 to twentyfold increase in the number of high-value stolen cards on black market websites, from nearly every bank and credit union." *See* "For Target, the Breach Numbers Grow," THE NEW YORK TIMES, Jan. 10, 2014, *available at* http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0 (attached hereto as Exhibit G).

19. As a direct and proximate result of the Target Data Breach, Plaintiff and members of the Class have been damaged, because Target's wrongful conduct has caused Class members to incur significant losses associated with credit and debit card cancellation and/or reissuance; customer reimbursement for fraud losses; lost interest and transaction fees; lost customers; administrative expenses associated with monitoring and preventing fraud and administrative expenses in dealing with customer confusion; and claims alleging fraudulent activity.

Target Data Retention Practices Violate Applicable Laws

20. Defendant, at all times relevant to this action, represented and had a duty to Plaintiff and members of the Class to: (a) properly secure credit card magnetic stripe information; (b) not retain or store such information subsequent to authorization of a transaction; and (c) not disclose such information to unauthorized third parties.

21. As outlined in numerous reports, Defendant retained magnetic stripe information and data from millions of credit and debit cards issued by Plaintiff and members of the Class.

22. Defendant negligently allowed credit card magnetic stripe information to be compromised.

23. Upon information and belief, Defendant negligently utilized a computer system that retained, stored, and/or disclosed (or allowed to be disclosed) credit card magnetic stripe information.

24. Data from the magnetic stripe on millions of credit cards, issued by banks and credit unions to their customers and members, was used by those customers at Target stores, and was accessed or obtained by third parties from Defendant.

25. Third parties were able to access, obtain, and use the credit card magnetic stripe information to fraudulently make transactions and to sell, transfer, use, or attempt to use such information for fraudulent purposes.

26. As a result of the events detailed herein, Plaintiff and members of the Class have been and continue to be forced to protect their members and avoid fraud losses by cancelling and reissuing cards with new account numbers and magnetic stripe information.

27. As a result of Defendant's failure to safeguard customer information, to date, Plaintiff has been forced to cancel and reissue approximately 75 cards and incur related costs for notification and reissuance of cards to its members.

28. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the Class. Moreover, as a result of the events detailed herein, Plaintiff and members of the Class suffered losses resulting from the Target Data Breach related to: (a) reimbursement of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as cancelling compromised cards and purchasing and mailing new cards to their members.

29. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

CLASS ACTION ALLEGATIONS

30. Plaintiff brings this action on its own and on behalf of all other credit unions similarly situated. The proposed class is defined as:

> All banks, credit unions and other financial institutions in the United States, that as a result of the Target security breach, were forced to communicate with their customers, close out or open new customer accounts, reissue credit and/or debit cards, absorb

unauthorized charges to members' accounts, or were in any other way forced to pay for issues related to the Target security breach (the "Class").

31. Plaintiff First Choice Federal Credit Union is a member of the Class it seeks to represent.

32. The Class is so numerous that joinder of all members is impracticable.

33. The members of the Class are readily ascertainable.

34. Plaintiff's claims are typical of the claims of all members of the Class.

35. The conduct of Defendant has caused injury to Plaintiff and members of the Class.

36. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendant.

37. Plaintiff will fairly and adequately represent the interests of the Class.

38. Plaintiff is represented by experienced counsel who are qualified to litigate this case.

39. Common questions of law and fact predominate over individualized questions. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

40. There are questions of law and fact common to all members of the Class, the answers to which will advance the resolution of the claims of the Class members and that include, without limitation:

a) Whether Defendant failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;

b) Whether the conduct of Defendant resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;

c) Whether Defendant improperly retained customer personal and financial information despite representations that it would not keep such information;

d) Whether Defendant disclosed, either directly or indirectly, the private financial information of customers;

e) Whether Defendant violated Minn. Stat. Ann. §325E.64;

f) Whether Defendant engaged in unfair and deceptive acts or practices as set forth in Minn. Stat. Ann. §325F.69 Subd. 1;

g) Whether Plaintiff and members of the Class have been injured by Defendant's violations of Minnesota law;

h) Whether Plaintiff and members of the Class are entitled to injunctive relief; and

i) Whether Plaintiff and members of the Class are entitled to damages and the measure of such damages.

COUNT ONE
VIOLATION OF MINN. STAT. ANN. § 325F.69 SUBD. 1

41. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

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

43. Plaintiff and members of the Class are credit unions engaged in trade or commerce.

44. Upon information and belief, Defendant's computer systems that process and store information related to credit and debit card transactions on which customer data was

retained and from which customer data was improperly accessed are located in Minneapolis, Minnesota.

45. Defendant's practice of retaining, failing to safeguard, and allowing access to confidential customer data constitutes deceptive acts and unfair trade practices within the meaning of Minn. Stat. Ann. §325F.69 Subd. 1.

46. Defendant's actions in connection with its failures to adequately protect its customers' data, and its misconduct regarding the confidential debit and credit cardholders' information constitute deceptive acts and unfair trade practices, having a direct and substantial effect in Minnesota and throughout the United States causing substantial damages to Plaintiff and members of the Class.

COUNT TWO
VIOLATION OF MINN. STAT. ANN. § 325E.64

47. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

48. Defendant had a duty under Minn. Stat. Ann. § 325E.64 Subd. 2, to provide notification of the data breach to Plaintiff and members of the Class. The statute specifically requires that:

> No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

49. Minn. Stat. Ann. § 325E.64 Subd. 3 details Defendant's responsibilities following the breach. Specifically, this subdivision provides that:

> Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:
>
> (1) the cancellation or reissuance of any access device affected by the breach;
>
> (2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;
>
> (3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;
>
> (4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and
>
> (5) the notification of cardholders affected by the breach.
>
> The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

50. Defendant breached the duties it owed to Plaintiff and members of the Class under Minn. Stat. Ann. § 325E.64 by failing to remove or delete card security code data, the PIN verification code number, and/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.

51. As a direct and proximate result of Defendant's breach of its duties under Minn. Stat. Ann. § 325E.64, Plaintiff and members of the Class have suffered substantial losses as detailed herein.

COUNT THREE
NEGLIGENCE

52. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

53. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining and retaining their members' personal and financial information.

54. Defendant owed a duty to Plaintiff and the Class to provide adequate security to protect their members' personal and financial information.

55. Defendant breached its duties, by (1) retaining customer data beyond the period allowed under Minn. Stat. Ann. § 325E.64; (2) allowing an unlawful intrusion into its computer system; (3) failing to protect against such an intrusion; and (4) allowing the personal and financial information of customers from Plaintiff and the Class to be accessed by third parties.

56. Defendant knew, or should have known, of the risks inherent in retaining such information, and the importance of providing adequate security.

57. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered substantial losses as detailed herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendant and in favor of Plaintiff and the Class and award the following relief:

A. That this action be certified as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as representative of the Class and Plaintiff's counsel as counsel for the Class;

B. Monetary damages;

C. Damages pursuant to Defendant's willful and knowing violations of Minn. Stat. Ann. § 325F.69 Subd. 1;

D. A finding that Defendant violated Minn. Stat. Ann. §325E.64 and an order enjoining Defendant from any further improper retention of customer data;

E. Reasonable attorneys' fees and expenses, including those related to experts and consultants;

F. Costs;

G. Pre and post judgment interest; and

H. Such other relief as this Court may deem just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff, individually and on behalf of the Class, demands a trial by jury for all issues so triable.

DATED: January 31, 2014

Respectfully submitted,

/s/ Gary F. Lynch
Gary F. Lynch
CARLSON LYNCH LTD
R. Bruce Carlson
Jamisen Etzel
PNC Park
115 Federal Street, Suite 210
Pittsburgh, PA 15212
Tel: (412) 322-9243
Fax: (412) 231-0246

Benjamin J. Sweet
Edwin J. Kilpela, Jr.
DEL SOLE CAVANAUGH STROYD LLC
200 First Avenue, Suite 300
Pittsburgh, PA 15222

Tel: (412) 261-2393
Fax: (412) 261-2110

Shanon J. Carson (PA 85957)
Alexandra L. Koropey (PA 315240)
BERGER & MONTAGUE, P.C.
1622 Locust Street
Philadelphia, PA 19103
Tel: (215) 875-4656
Fax: (215) 875-4604