IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FIRST CHOICE FEDERAL CREDIT UNION, individually and on behalf of a class of similarly situated financial institutions, Plaintiff, v. THE HOME DEPOT, INC., Defendant.	Case No: 1:14-cv-2975-AT **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff First Choice Federal Credit Union ("Plaintiff"), through its undersigned counsel, individually and on behalf of a class of similarly situated financial institutions, files this Class Action Complaint against Defendant The Home Depot, Inc. ("Home Depot" or "Defendant"), and states the following:

INTRODUCTION

1. This is a class action on behalf of credit unions, banks, and other financial institutions that suffered injury as a result of a massive security breach beginning in approximately April, 2014 and compromising Home Depot's store customers' names, credit and debit card numbers, card expiration dates, and card verification values ("CVVs"), as well as the states and ZIP codes of the stores

associated with individual card transactions (hereinafter, the "Home Depot Data Breach").

2. The Home Depot Data Breach will require Plaintiff and other financial institutions to: (a) cancel or reissue any access device affected by the Home Depot Data Breach; (b) close any deposit, transaction, checking, 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, checking, or other accounts affected by the Home Depot Data Breach; (d) refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Home Depot Data Breach; (e) notify cardholders affected by the Home Depot Data Breach; (f) respond to a higher volume of cardholder complaints, confusion, and concern; and (g) increase fraud monitoring efforts. Plaintiff has already incurred the cost of cancelling/reissuing numerous debit cards for its customers affected by the Home Depot Data Breach.

3. In addition, the Home Depot Data Breach has caused, and will continue to cause, Plaintiff and the Class to lose revenue as a result of a decrease in card usage after the breach was disclosed to the public.

4. As alleged herein, the injuries to Plaintiff and the Class are being directly 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 and store location information. Defendant failed to take adequate security measures despite well-publicized data breaches at large, national retail and restaurant chains in recent months, including Target, Sally Beauty, Harbor Freight Tools, and P.F. Chang's.

5. The attack underlying the Home Depot Data Breach involved mostly the same techniques as those used in other major data breaches in the preceding months and year. Despite having knowledge that such data breaches were occurring throughout the retail industry, Home Depot failed to properly defend sensitive payment card information from what is now a well-known, preventable angle of attack.

6. In addition to failing to prevent the attack in the first instance, Home Depot failed to detect the attack for a period of approximately four months. In fact, Home Depot only learned of the breach from law enforcement and financial institutions. Therefore the volume of data stolen was much greater than it would have been had Home Depot monitored its data security adequately enough to identify and eliminate the attack as it was occurring.

7. As a result of Home Depot's negligence, vast amounts of customer information were stolen from Home Depot's computer network. Millions of Home

Depot'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. As a direct consequence, Plaintiff and members of the Class have incurred and will continue to incur significant costs associated with, among other things, notifying their customers of issues related to the Home Depot Data Breach, closing out and opening new customer accounts, reissuing customers' cards, and/or refunding customers' losses resulting from the unauthorized use of their accounts. Additionally, Plaintiff and members of the Class have suffered and will continue to suffer lost revenues as a result of decreased usage of their customers' debit/credit cards.

8. Plaintiff and the Class seek to recover damages caused by Defendant's negligence, as set forth herein.

JURISDICTION AND VENUE

9. 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 which are citizens of a different state than Defendant, including named Plaintiff First Choice Federal Credit Union, which is a citizen of Pennsylvania. Defendant Home Depot is a citizen of

Delaware, where it is incorporated, and Georgia, where its principal place of business is located.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because Defendant Home Depot resides in this judicial district, regularly transacts business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

PARTIES

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

12. Defendant The Home Depot, Inc. is a Delaware corporation with its principal place of business located in Atlanta, Georgia. Home Depot operates a chain of retail stores that sell a wide variety of merchandise, including tools, home goods, and construction supplies. Home Depot operates over 2,200 stores in the United States.

FACTUAL BACKGROUND

Background on Electronic Debit and Credit Card Transactions

13. Plaintiff and the members of the Class are financial institutions that issue payment cards, including debit and credit cards, and/or perform, facilitate, or support card issuing services on behalf of their customers. Plaintiff's customers used

these payment cards to make purchases at Home Depot stores during the period of the Home Depot Data Breach.

14. Home Depot stores accept customer payment cards for the purchase of goods and services. At the point of sale ("POS"), these cards are swiped on a POS terminal, and a personal identification number or some other confirmation number is entered, or a receipt is signed to finish the transaction on behalf of the customer.

15. In basic terms, the other side of the transaction continues as follows: When the card is swiped, the merchant (*e.g.* Home Depot) uses the payment processing networks (*e.g.* Visa or MasterCard) to transmit a request for authorization to the institution which issued the payment card (*e.g.* Plaintiff). If the issuing institution authorizes the payment, the merchant electronically forwards a receipt of the transaction to another financial institution known as the "acquiring bank," which contracts with the merchant to process credit and debit card transactions. The acquiring bank forwards the funds to the merchant to satisfy the transaction, and is then reimbursed by the card-issuing institution (Plaintiff). The issuing institution posts the debit or credit transaction to its customer's account.

16. Given the extensive network of financial institutions involved in these transactions and the sheer volume of daily transactions using credit and debit cards, it is unsurprising that financial institutions and credit card processing companies

have issued rules and standards governing the basic measures that merchants must take to ensure consumers' valuable data is protected. First, the card processing networks issue regulations ("Card Operating Regulations") that are enforceable upon Home Depot as a condition of Home Depot's contract with its acquiring bank. The Card Operating Regulations prohibit Home Depot (or any merchant) from disclosing any cardholder account numbers, personal information, magnetic stripe information, or transaction information to third parties other than the merchant's agent, the acquiring bank, or the acquiring bank's agents. Under the Card Operating Regulations, Home Depot was required to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and protect it from unauthorized disclosure.

17. Similarly, the Payment Card Industry Data Security Standards ("PCI DSS") are a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. They apply to all organizations and environments where cardholder data is stored, processed or transmitted and require merchants like Home Depot to 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. As part of Home Depot's agreements

with Visa and MasterCard, Home Depot represented that it would be compliant with PCI DSS. The twelve requirements are:

Build and Maintain a Secure Network

1) Install and maintain a firewall configuration to protect cardholder data

2) Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3) Protect stored cardholder data

4) Encrypt transmission of cardholder data and sensitive information across open, public networks

Maintain a Vulnerability Management Program

5) Protect all systems against malware and regularly update anti-virus software or programs

6) Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7) Restrict access to cardholder data by business need-to-know

8) Identify and authenticate access to system components

9) Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10) Track and monitor all access to network resources and cardholder data

11) Regularly test security systems and processes

Maintain an Information Security Policy

12) Maintain a policy that addresses information security for all personnel[1]

18. Home Depot was at all times fully aware of its data protection obligations, which emanated from its participation in the payment card processing networks and its daily collection and transmission of tens of thousands of sets of payment card data.

19. As a result of its participation in the payment card processing networks, Home Depot knew that, in each instance when it accepted payment cards for a purchase at one of its stores, its customers and the financial institutions which issued the payment cards to the customers were trusting that Home Depot would keep its customers' sensitive financial information secure from would-be data thieves.

20. Moreover, Home Depot knew that if it failed to secure its customers' sensitive financial information, the financial institutions issuing the payment cards to its customers, i.e., Plaintiff and the members of the class, would suffer harm in the form of having to notify customers, close out and open new customer accounts, reissue customers' cards, and/or refund customers' losses resulting from the unauthorized use of their accounts, and additionally, suffer lost revenues as a result of decreased usage of their customers' debit/credit cards.

[1] The PCI DSS 12 core security standards can be found here: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf, at pg. 5 (last visited Sept. 9, 2013).

The Home Depot Data Breach: Initially Discovered and Disclosed By Others

21. On September 2, 2014, respected data security blogger Brian Krebs reported that "Multiple banks say they are seeing evidence that Home Depot stores may be the source of a massive new batch of stolen credit and debit cards that went on sale this morning in the cybercrime underground."[2]

22. Home Depot said at that time only that it was "looking into some unusual activity," and that it was not ready to confirm that a data breach had occurred.[3]

23. On September 8, 2014, Home Depot confirmed the breach and revealed that the breach may have affected any customer at any Home Depot store in the United States and Canada who made in-store purchases between April, 2014 and early September, 2014. Home Depot further indicated that it was not aware of the breach until it received notification from banks and law enforcement on September 2, 2014.[4]

24. After gaining access to Defendant's networks, hackers employed

---

[2] *See* Krebs on Security, "Banks: Credit Card Breach at Home Depot," Sept. 2, 2014 (*available at* http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/).

[3] *Id.*

[4] *See* https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf

"RAM scraper" malware, similar to that used in the Target data breach of 2013, to gain access to the sensitive personal and financial information of consumers.[5]

25. The RAM scraper malware was installed on Home Depot POS terminals and Home Depot failed to detect its installation and/or failed to take appropriate steps to eliminate it.[6] Following the installation of the RAM scraping malware, hackers were able to harvest consumer information from multiple POS locations.

26. Hackers used RAM scraper malware to harvest this unencrypted information. This information was then gathered and stored on the infiltrated network and thereafter shipped in batches to external servers, controlled by the hackers.

27. The New York Times has reported, and other private security companies have confirmed, that the breach could affect upwards of 60 million

[5] *See* http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/#more-27751.

[6] RAM scraper malware works as follows. When a card is swiped or entered at a POS terminal, the terminal processes the card data unencrypted on its random access memory ("RAM") for a short time. Hackers use RAM scraper malware, the type of malware installed on Home Depot's POS terminals, to harvest this unencrypted information.

credit/debit card accounts.[7]

28. BillGuard, a private security firm, used calculations drawn from over one million active card accounts on its website and sixteen data breaches in the past year to estimate that the accounts compromised in the Home Depot Data Breach could result in $2–3 billion in fraudulent charges.[8]

The Hackers Were Able to Access Home Depot's POS Terminals As A Result of Home Depot's Lax Security Measures

29. Upon information and belief, Home Depot utilized weak password configurations and did not employ lockout security procedures[9] at its remote access points.

30. The failure to utilize lockout security procedures allowed hackers to utilize high-speed computers to gain access to Home Depot's system by guessing random combinations of usernames and passwords until a matching combination was found.

---

[7] *See* http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_r=0; *see also* http://blog.billguard.com/2014/09/home-depot-data-breach-estimated-impact/.

[8] *See* http://blog.billguard.com/2014/09/home-depot-data-breach-estimated-impact/.

[9] Lockout security procedures thwart hacker attempts to guess usernames and passwords by locking out IT addresses when multiple failed login attempts occur.

31. Upon information and belief, Home Depot also failed to segregate its POS networks from its larger corporate IT networks.

32. Home Depot's failure to isolate its POS network allowed hackers to gain access to Home Depot's entire corporate IT network and obtain massive amounts of consumer information.

33. Reputable media reports describe numerous deficiencies within Home Depot's IT security department. A Bloomberg Businessweek report, relying on interviews with former Home Depot employees, identified the following problems with Home Depot's approach to IT security: 1) Home Depot's payment systems were not configured to properly encrypt customer payment card data; 2) Home Depot's IT department experienced high employee turnover; 3) Home Depot was using outdated malware detection programs, including a seven-year-old Symantec program, Endpoint Protection 11; 4) Although Symantec released a new version of the program in 2011, Home Depot did not switch to the new program, even though Symantec has been phasing out user support for Endpoint Protection 11 and publicly announced it would end all support for it by January 2015; and 5) Home Depot IT personnel informed upper level executives that the company's security was inadequate and requested that the company take more extensive action to protect its

payment processing systems, but the superior officers denied those requests and stated that the company would settle for "C-level security."[10]

34. Upon information and belief, Home Depot's IT department and executives were aware that the company was vulnerable to an attack of the same nature as the one directed against Target in late 2013, and they were aware of countermeasures on the market which could reduce or eliminate the ability of attackers to steal customer card data from POS terminals. Nevertheless, Home Depot did not act in time to prevent the Home Depot Data Breach.

Home Depot Should Have Recognized the Flaws in its Security System and Should Have Been Alerted to the Threat of RAM Scraper Malware

35. Data breaches are preventable.

36. The Online Trust Alliance, a non-profit organization whose mission is to enhance online trust, user empowerment and innovation, in its 2014 annual report, estimated that 740 million records were stolen in 2013 and that 89% of data breaches occurring in that year were avoidable.

[10] *See* http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say

37. The deficiencies in Home Depot's security system include a lack of elementary security measures that even the most inexperienced IT professional would identify as problematic.

38. The security flaws outlined above, along with many others, were explicitly highlighted by VISA, as early as 2009, when it issued a Data Security Alert describing the threat of RAM scraper malware.[11] The report instructs companies to "secure remote access connectivity," "implement secure network configuration, including egress and ingress filtering to only allow the ports/services necessary to conduct business" (i.e. segregate networks), "actively monitor logs of network components, including intrusion detection systems and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses," "encrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit" and "work with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration."

39. Home Depot's security flaws run afoul of best practices and industry standards. More specifically, the security practices in place at Home Depot are in

[11] The report can be found at: https://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf (last visited Sept. 9, 2014).

stark contrast and directly conflict with the PCI DSS and the twelve PCI DSS core security standards. All merchants are required to adhere to the PCI DSS as members of the payment card industry.

40. As a result, industry practice, the PCI DSS, and well-documented past data breaches alerted Home Depot to the risk associated with their lax security protocols.

Home Depot Had a Duty to Plaintiffs to Prevent the Data Breach

41. RAM scraper malware has been used to attack POS terminals since 2011.

42. RAM scraper malware has been used recently to attack large retailers such as Target, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu.

43. Home Depot was aware that RAM scraper malware is a real threat and is a primary tool of attack used by hackers.

44. The U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, has also alerted retailers to the threat of POS malware, and on July 31, 2014 issued a guide for retailers on protecting against the threat of POS malware.[12]

[12] https://www.us-cert.gov/ncas/alerts/TA14-212A

45. Despite the fact that Home Depot was put on notice of the very real possibility of consumer data theft associated with its security practices and despite the fact that Home Depot knew or, at the very least, should have known about the elementary infirmities associated with its security systems, it still failed to make changes to its security practices and protocols.

46. Home Depot knew that failing to protect customer card data would cause harm to the card-issuing institutions such as Plaintiff and the Class, because the issuers are financially responsible for fraudulent card activity and must incur significant costs to prevent additional fraud.

47. Indeed, Home Depot's public statements to customers after the data breach plainly state Home Depot's belief that card-issuing institutions "are responsible" for fraudulent charges on cardholder accounts resulting from the data breach.[13]

48. Home Depot, at all times relevant to this action, had a duty to Plaintiff and members of the Class to, and represented that it would: (a) properly secure payment card magnetic stripe information at the point of sale and on Home Depot's

[13] *See* Home Depot, "FAQs," Sept. 8, 2014, *available at* https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf ("First, you will not be responsible for any possible fraudulent charges. The financial institution that issued your card or The Home Depot are responsible for those charges.").

internal networks; (b) encrypt payment card data using industry standard methods; (c) use available technology to defend its POS terminals from well-known methods of attack; and (d) act reasonably to prevent the foreseeable harms to Plaintiff and the Class which would naturally result from payment card data theft.

49. Defendant negligently allowed payment card magnetic stripe information and geographical location information to be compromised by failing to take reasonable steps against an obvious threat.

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

51. The cancellation and reissuance of cards is resulting 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 have suffered and will continue to suffer losses resulting from the Home Depot 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 customers.

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

CLASS ACTION ALLEGATIONS

53. Plaintiff brings this action individually and on behalf of all other financial institutions similarly situated pursuant to Fed. R. Civ. P. 23. The proposed class is defined as:

> All Financial institutions—including, but not limited to, banks and credit unions—in the United States (including its Territories and the District of Columbia) that issue payment cards, including credit and debit cards, or perform, facilitate, or support card issuing services, whose customers made purchases from Home Depot stores from April 1, 2014 to the present[14] (the "Class").

54. Plaintiff is a member of the Class it seeks to represent.

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

56. The members of the Class are readily ascertainable.

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

[14] At this time, it is unknown when or if the Home Depot Data Breach has ended. As the litigation progresses, the class definition may be amended as necessary to reflect the proper timeframe, when that information becomes available.

58. The conduct of Defendant has caused injury to Plaintiff and members of the Class in substantially the same ways.

59. 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.

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

61. Defendant has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

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

63. 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.

64. 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 failed to encrypt customer payment card data;

d) Whether Defendant improperly retained customer personal and financial information or allowed such information to be retained on its systems;

e) Whether Defendant's actions were negligent;

f) Whether Defendant owed a duty to Plaintiff and the Class;

g) Whether the harm to Plaintiff and the Class was foreseeable;

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
NEGLIGENCE

65. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

66. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining and processing Plaintiff's customers' personal and financial information.

67. Defendant owed a duty to Plaintiff and the Class to provide adequate security to protect their mutual customers' personal and financial information.

68. Defendant breached its duties by (1) allowing a third-party intrusion into its computer systems; (2) failing to protect against such an intrusion; (3) failing to detect the intrusion for a period of four or more months; (4) allowing the personal and financial information of customers of Plaintiff and the Class to be accessed by third parties on a massive scale.

69. Defendant knew or should have known of the risk that its POS terminals could be attacked using methods similar or identical to those previously used against major retailers in recent months and years.

70. Defendant knew or should have known that its failure to take reasonable measures to protect its POS terminals against obvious risks would result in harm to Plaintiff and the Class.

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

COUNT TWO

NEGLIGENT MISREPRESENTATION BY OMISSION

72. Plaintiff incorporates and re-alleges all allegations above as if fully set forth herein.

73. Through its acceptance of credit and debit payment cards and participation in the payment card processing system, Home Depot held itself out to Plaintiff and the Class as possessing and maintaining adequate data security measures and systems that were sufficient to protect the personal and financial information of shoppers using credit and debit cards issued by Plaintiff and the Class.

74. Home Depot further represented that it would secure and protect the personal and financial information of shoppers using credit and debit cards issued by Plaintiff and the Class by agreeing to comply with both Card Operating Regulations and the PCI DSS.

75. Home Depot knew or should have known that it was not in compliance with the requirements of Card Operating Regulations and the PCI DSS.

76. Home Depot knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith required it to disclose to Plaintiff and the Class.

77. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to Plaintiff and the Class.

78. Home Depot also failed to exercise reasonable care when it failed to timely communicate information concerning the data breach that it knew, or should have known, compromised the personal and financial information of customers using credit and debit cards issued by Plaintiff and the Class.

79. Home Depot's failure to disclose its inadequate security systems was particularly egregious in light of the highly publicized, similar data breaches at other national retailers in the months preceding the Home Depot Data Breach.

80. Had Plaintiff and the Class known that Home Depot was not compliant with the Card Operating Regulations and the PCI DSS, Plaintiff and the Class would have either taken action to prevent their cards from being used for electronically processed purchases at Home Depot or required Home Depot to take immediate corrective action.

81. As a direct and proximate result of Home Depot's negligent misrepresentation by omission, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

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. Injunctive Relief;

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

E. Costs;

F. Pre- and post- judgment interest; and

G. 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: September 16, 2014

Respectfully submitted,

By: /s/ Thomas A. Withers
Thomas A. Withers
Georgia Bar No. 772250
GILLEN WITHERS & LAKE, LLC
8 East Liberty Street
Savannah, Georgia 31412
Tel: (912) 447-8400
Fax: (912) 233-6584
twithers@gwllawfirm.com

Gary F. Lynch
Edwin J. Kilpela
Jamisen Etzel
(all to be admitted *pro hac vice*)
CARLSON LYNCH SWEET & KILPELA, LLP
PNC Park
115 Federal Street, Suite 210
Pittsburgh, PA 15212
Tel: (412) 322-9243
Fax: (412) 231-0246
glynch@carlsonlynch.com
ekilpela@carlsonlynch.com
jetzel@carlsonlynch.com

Richard A. Lockridge
Robert K. Shelquist
Karen Hanson Riebel
Heidi M. Silton
Eric N. Linsk
(all to be admitted *pro hac vice*)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 339-0981
ralockridge@locklaw.com
rkshelquist@locklaw.com
khriebel@locklaw.com
hmsilton@locklaw.com
rnlinsk@locklaw.com

Attorneys for Plaintiff

CERTIFICATION

The undersigned hereby certifies, pursuant to Local Civil Rule 7.1D, that the foregoing document has been prepared with one of the font and point selections (Times New Roman, 14 point) approved by the Court in Local Civil Rule 5.1B.

/s/ Thomas A. Withers
Thomas A. Withers
Georgia Bar No. 772250
GILLEN WITHERS & LAKE, LLC
8 East Liberty Street
Savannah, Georgia 31412
Tel: (912) 447-8400
Fax: (912) 233-6584
twithers@gwllawfirm.com

JS44 (Rev. 1/13 NDGA)

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

FIRST CHOICE FEDERAL CREDIT UNION, individually and on behalf of a class of similarly situated financial institutions

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Lawrence County, Pennsylvania
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANT(S)

THE HOME DEPOT, INC.

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Cobb
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

Thomas A. Withers
GILLEN WITHERS & LAKE, LLC
8 East Liberty Street
Savannah, Georgia 31412
Tel: (912) 447-8400
twithers@gwllawfirm.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION
(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
- ■ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- ☐ 2 U.S. GOVERNMENT DEFENDANT
- ☐ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES
(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☐ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☐ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. ORIGIN (PLACE AN "X "IN ONE BOX ONLY)

■ 1 ORIGINAL PROCEEDING ☐ 2 REMOVED FROM STATE COURT ☐ 3 REMANDED FROM APPELLATE COURT ☐ 4 REINSTATED OR REOPENED ☐ 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District) ☐ 6 MULTIDISTRICT LITIGATION ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

The Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The cause is a class tort cause arising out of defendant's massive data breach, which resulted in the theft of customers' names, credit and debit card numbers, card expiration dates, and card verification values.

(IF COMPLEX, CHECK REASON BELOW)

- ☐ 1. Unusually large number of parties.
- ☐ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP)_____

JUDGE_____ MAG. JUDGE_____ NATURE OF SUIT_____ CAUSE OF ACTION_____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK
- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☐ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☑ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 444 WELFARE
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☐ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $** to be proven at trial

JURY DEMAND ☐ **YES** ☐ **NO** **(CHECK YES ONLY IF DEMANDED IN COMPLAINT)**

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE_____ **DOCKET NO.**_____

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**
- ☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

/s/ Thomas Withers — 9/16/2014

SIGNATURE OF ATTORNEY OF RECORD **DATE**