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

GREATER CHAUTAQUA FEDERAL CREDIT UNION, individually and on behalf of all others similarly situated, Plaintiff, v. HOME DEPOT U.S.A., INC. Defendant.	)	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Greater Chautauqua Federal Credit Union, individually and on behalf of similarly situated financial institutions, files this Class Action Complaint against Defendant Home Depot U.S.A., Inc. ("Defendant" or "Home Depot").

NATURE OF THE CASE

1. Plaintiff brings this class action against Home Depot for its failure to secure and safeguard its customers' personal and private financial information.

2. In or around April 2014, computer hackers began using malicious software to access point-of-sale systems at Home Depot store locations throughout the U.S. and Canada. The hackers stole many customers' debit and credit card

information, including card numbers, account holders' names, and the address of the Home Depot store where the card was used. In or around September 2014, this information was offered for sale on "rescator.cc," an underground web site known for trafficking in stolen card information.

3. Home Depot's negligent security lapses enabled the theft of its customers' financial information, as well as subsequent fraudulent charges on their debit and credit cards. Home Depot claims that it did not become aware of any potential security breach until September 2, 2014, approximately *five months* after the breach began. This lapse occurred despite similar recent, high-profile security breaches at other major retailers including Target and Neiman Marcus. During this time, customers' personal and private financial information lay exposed to sale on the black market.

4. Nearly a week after learning of the breach, on or around September 8, 2014, Home Depot finally acknowledged that the breach had occurred and that millions of customers' financial information had been compromised.

5. As a direct result of Home Depot's negligent security failures, Plaintiff and the Class have incurred significant damages totaling in the hundreds of millions of dollars, including but not limited to: reissuing debit and credit cards, loss of customers, costs of covering fraudulent charges, notifying customers of the

breach, and handling customer service inquiries and investigations related to the breach. According to a recent survey conducted by the Credit Union National Association, it is estimated that, for credit unions alone, 7.2 million cards were affected and credit unions incurred $60 million in direct costs. Those figures do not include the additional costs incurred by other types of financial institution Class members and represent only a fraction of damages to the Class.

6. Accordingly, Plaintiff, individually and on behalf of the Class, asserts claims against Home Depot for negligence, negligence *per se*, and negligent material omission.

JURISDICTION AND VENUE

7. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual Class members exceed the sum or value of $5,000,000, exclusive of interests and costs. Further, Plaintiff and many Class members are citizens of a different state than the Defendant.

8. Personal jurisdiction over Home Depot in this Court is proper and necessary because Home Depot maintains its principal headquarters in Georgia, is registered to conduct business in Georgia, and has sufficient minimum contacts in Georgia. Home Depot intentionally avails itself of the Georgia consumer market

through the promotion, sale, marketing, and distribution of its products to Georgia residents.

9. Venue is proper in this District under 28 U.S.C. § 1391(a)-(d) because, among other things, Home Depot's principal place of business is in Georgia and a substantial part of the events giving rise to the Plaintiff's claims occurred in Georgia.

PARTIES

10. Plaintiff Greater Chautauqua Federal Credit Union is a chartered federal credit union whose main offices are located in Falconer, NY.

11. Plaintiff provided its customers with credit and/or debit cards equipped with magnetic strips containing sensitive financial data. Plaintiff's customers used these cards to engage in financial transactions with Home Depot stores.

12. As a result of the security breach, Plaintiff incurred damages for, among other things, the cost of replacement cards. These costs are ongoing, as Plaintiff continues to investigate fraudulent transactions caused by the data breach that have not yet been reimbursed.

13. Defendant Home Depot is a Delaware corporation with its principal place of business in Atlanta, Georgia. Home Depot is the world's largest home

improvement retailer, operating over 2,266 store locations throughout the United States, Canada, and Mexico.

FACTUAL BACKGROUND

Home Depot Ignored Industry Regulations and Failed to Implement Security Protocols for Customer Data.

14. Like the vast majority of retailers, Home Depot processes in-store debit and credit card payments for customer purchases.

15. Retailers, such as Home Depot, that process credit and debit transactions contract with an acquiring bank in order to do so. These contracts give merchants the ability to process credit and debit transactions.

16. When a Home Depot customer makes a purchase, Home Depot requests authorization for the transaction from an issuer (such as Plaintiff, or any other Class member). Once the issuer approves the transaction, Home Depot processes the transaction and passes on the purchase receipt to the acquiring bank with which it has contracted. Then, the acquiring bank will pay Home Depot for the purchase and forward the final transaction to the issuer, at which point the issuer sends payment to the acquiring bank. Once this process is complete, the issuer will post the purchase charge to the customer's credit or debit account.

17. Many payment processing networks, such as Visa and Mastercard, issue regulations ("Card Operating Regulations") that are binding on Home Depot,

as a condition of Home Depot's contract with its acquiring bank. The Card Operating Regulations prohibit Home Depot from disclosing 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. Home Depot was required under the Card Operating Regulations to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and to protect it from unauthorized disclosure.

18. Home Depot failed to comply with the Card Operating Regulations and failed to inform Plaintiff and the Class of its failure.

19. At the time of the breach, in order to process these types of transactions, Home Depot was also required to abide by the Payment Card Industry Data Security Standard (PCI DSS), industry-wide standards governing the security of financial information transmitted through debit and credit card purchases. On information and belief, PCI DSS compliance was required pursuant to Home Depot's contracts with acquiring banks. At the time of the breach, PCI DSS 2.0 was in effect. Home Depot represented to Class members and the public that it met all current standards for PCI DSS.

20. PCI DSS are not onerous; in fact, they generally represent only the most minimal precautions that should be taken to safeguard customer data.

21. PCI DSS requires merchants such as Home Depot to: (a) properly secure personal information stored on credit and debit cards; (b) not retain or store information contained on credit or debit cards beyond the time period necessary to authorize the transaction; (c) not disclose the information contained on credit or debit cards to third parties; and (d) track and monitor all access to network resources and cardholder data. Home Depot failed to abide by all of these standards.

22. PCI DSS required Home Depot to protect its customers' personal and financial data and to not disclose, or allow to be disclosed, any of this data to third parties.

23. Under the relevant PCI DSS, Home Depot should have implemented a security system that would protect sensitive customer data. Home Depot was required to install a firewall that would prevent external access to its computer systems, along with other electronic and physical barriers to customer data. The standards required restrictions on physical and electronic access to its computer systems so that only those who needed to access the system for a valid purpose were able to do so. The standards require the creation of passwords, use of

encryptions, and assignment of unique IDs to each individual with access to Home Depot's systems. Home Depot failed to abide by these standards and failed to inform Plaintiff and the Class of its failure.

24. PCI DSS required Home Depot to consistently monitor access to its computer networks and to any cardholder account data on its systems to ensure that any breaches that occurred could be caught and quickly dealt with. The standards called for regular tests to ensure proper operation of security protocols and regular reviews of logs for all system components. Home Depot failed to abide by these standards and failed to inform Plaintiff and the Class of its failure.

25. PCI DSS also required Home Depot not to maintain any cardholder data beyond the time period necessary to process a transaction.

26. Home Depot was fully aware of its obligations to protect its customers' personal financial data. Due to its participation in payment card processing networks, Home Depot knew that its customers and the financial institutions that issued cards to customers relied on Home Depot to adequately protect their personal financial data from unauthorized access.

27. Home Depot was fully aware that, in the instance that it failed to protect its customers' personal financial data, the financial institutions that issued cards to its customers would suffer injury, including being required to spend

substantial resources to notify customers, open and close cardholder accounts, reissue credit and debit cards, forgo interest and transaction fees, monitor and prevent additional fraud, and reimburse customers for fraudulent transactions.

After Months of Allowing Customer Data to Be Compromised, Home Depot Discovers the Breach

28. Home Depot has indicated that, until receiving notification from law enforcement and from Class members, it was not aware of any potential security breach. On its corporate website, Home Depot states that, on September 2, 2014, it first became aware of a breach involving the unauthorized access and theft of its customers' debit and credit card information.[1]

29. That same day, a large batch of debit and credit card data emerged for sale on "rescator.cc," an underground website known for marketing in stolen financial information. Rescator.cc is the website known for selling card information stolen in the highly publicized 2013 cyber attack on Target. Multiple banks offered evidence that Home Depot stores were the likely source of the stolen data. A security blogger named Brian Krebs posted evidence that the ZIP code

[1] *See* http://phx.corporate-ir.net/phoenix.zhtml?c=63646&p=RssLanding&cat=news&id=1964976 (last visited September 17, 2014).

data of the newly posted stolen data and the ZIP code data of the Home Depot stores shared a 99.4 percent overlap.[2]

30. Home Depot began an investigation into the breach, in tandem with the U.S. Secret Service and outside security firms. On September 8, 2014, Home Depot confirmed that customers' personal and private financial information had been compromised by the breach. It indicated that potential victims included anyone who used a debit or credit card at any one of Home Depot's over 2,000 retail locations in the U.S. or Canada since April 2014.

31. Upon information and belief, Home Depot's security systems used weak password configurations and failed to use lockout security procedures at remote access points. This failure enabled the hackers to gain access to Home Depot's corporate IT network.

32. After illicitly gaining access to Home Depot's networks, the hackers used "RAM scraper" malware to gain access to Home Depot customers' personal and financial information.

33. Home Depot failed to detect the installation of RAM scraping malware on its point-of-sale terminals and failed to take steps to eliminate it.

---

[2] *See* http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/ (last visited September 17, 2014).

34. The hackers used the RAM scraping malware to steal Home Depot's customers' personal and financial information and move it to external servers controlled by the hackers.

35. Home Depot was aware, or should have been aware, of the threat posed by RAM scraping malware. In 2009, VISA issued a Data Security Alert describing such a threat.[3] The Alert 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."

36. The media and private security companies have reported that the security breach could affect over sixty million credit card accounts, twenty million

[3] *See* https://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf.

more than were affected by the 2013 Target breach.[4] Further, a survey of credit unions has found that damages may double those from the Target breach.

37. Home Depot did not inform Plaintiff and the Class about its deficient security systems. Plaintiff and Class members reasonably expected that Home Depot would safeguard confidential customer financial and personal information.

38. Indeed, despite the breach occurring over a months-long period, Home Depot was not even the first to report the security breach; security blogger Brian Krebs was.

Plaintiff and Class Members Suffered Damages Due to Home Depot's Failure to Adequately Secure Sensitive Customer Financial Information.

39. As a result of the data breach, Plaintiff and Class members have incurred significant financial costs by, among other things, cancelling and reissuing credit and debit cards, notifying customers, closing and opening accounts, lost interest and transaction fees, lost customers, covering fraudulent transactions, and the expenses associated with monitoring and preventing further fraud.

40. Home Depot failed to follow industry standards and did not effectively monitor its security systems to ensure the safety of customer

[4] *See* http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1.

information. As a result of its substandard security protocols, improper retention of cardholder data, and failure to regularly monitor for unauthorized access, the sensitive financial and personal data of Home Depot's customers was compromised for weeks with no warning to Plaintiff or members of the Class.

41. The security breach of Home Depot's systems was preventable.

42. Several former Home Depot employees, wishing to remain anonymous, have described a work environment involving "C-level security" (as opposed to A-level or B-level), which adversely impacted their IT security effectiveness.[5]

43. A "health check" on Home Depot's information systems, performed by Symantec employees in July 2014, revealed that Home Depot was using out-of-date malware detection systems. At this point, hackers may have been accessing customers' personal and financial data.

44. Three former Home Depot information security managers have stated that Home Depot was also using out-of-date antivirus software for its point-of-sale systems. Symantec released version 12 of its Endpoint Protection program in

[5] *See* http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say (last visited September 17, 2014).

2011, stating that the "threat landscape has changed significantly" and that version 12 would protect against the "explosion in malware scope and complexity."[6]

45. Despite the release of Endpoint Protection 12, Home Depot continued to use seven year-old version 11, despite security staffers' pleas to executives and despite Symantec's phasing out of user support for version 11.[7]

46. Home Depot has admitted that it was bound by applicable security standards, including PCI DSS, and that it was required to create and monitor a secure computer system that protected the personal and financial data contained on customer credit and debit cards. Home Depot further knew, or should have known, that it was required to delete all cardholder data, and not allow it to be accessed by third parties. Home Depot knew, or should have known, that it was required to regularly monitor its system to ensure the safety of sensitive customer data.

47. Further, Home Depot had a duty to Plaintiff and the Class to comply with card operating regulations, secure cardholder personal and financial information, not retain or store cardholder information longer than necessary to process transactions, and not disclose or allow such information to be disclosed to third parties.

---

[6] *See id.*
[7] *See id.*

48. Home Depot breached these duties and negligently allowed sensitive cardholder data to be compromised.

49. As a result of the data breach, Plaintiff and Class members were required and will continue to be required to spend substantial resources to notify customers, open and close cardholder accounts, reissue credit and debit cards, forgo interest and transaction fees, monitor and prevent additional fraud, and reimburse customers for fraudulent transactions.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action pursuant to Rules 23(a), 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure, individually and on behalf of a class defined as:

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issue payment cards (including debit or credit cards), or perform, facilitate, or support card issuing services, whose customers made purchases from Home Depot stores during the period from April 1, 2014 to the present[8] (the "Class").

[8] Plaintiffs may amend the Class definition as new details emerge regarding whether and when the breach has ended.

51. Excluded from the Class are: Home Depot, Inc., its affiliates, employees, officers and directors, the judge(s) assigned to this case, and the attorneys of record in this case.

52. The members of the Class are readily ascertainable.

53. The members of the Class are so numerous that joinder of all members would be impracticable.

54. There are common questions of law and fact that predominate over any questions affecting only individual Class members. These common legal and factual questions, include, but are not limited to:

a. Whether Home Depot owed a duty to Plaintiff and the Class members to protect cardholder personal and financial data;

b. Whether Home Depot failed to provide adequate security to protect consumer cardholder personal and financial data;

c. Whether Home Depot negligently or otherwise improperly allowed cardholder personal and financial data to be accessed by third parties;

d. Whether Home Depot failed to adequately notify Plaintiff and Class members that its data system was breached;

e. Whether Home Depot negligently misrepresented that it would abide by industry standards and regulations to protect cardholder data;

f. Whether Plaintiff and Class members suffered financial injury;

g. Whether Home Depot's failure to provide adequate security proximately caused Plaintiff and Class members' injuries;

h. Whether Plaintiff and Class members are entitled to damages and, if so, what is the measure of such damages; and

i. Whether Plaintiff and Class members are entitled to injunctive relief.

55. Plaintiff's claims are typical of the claims of the other Class members. Plaintiff and each of the other Class members are financial institutions who have been injured by Home Depot's security breach. Plaintiff's claims arise from the same practices and course of conduct that give rise to the other Class members' claims and are based on the same legal theories.

56. Plaintiff will fully and adequately assert and protect the interests of the other Class members. In addition, Plaintiff has retained class counsel who are experienced and qualified in prosecuting class action cases similar to this one.

Neither Plaintiff nor its attorneys have any interests contrary to or conflicting with other Class members' interests.

57. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the other Class members' claims is economically infeasible and procedurally impracticable. Class members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Further, Class treatment will also permit some smaller class members to litigate their claims where it would otherwise be too expensive or inefficient to do so. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

58. Home Depot has, or has access to, addresses and other contact information for the Class members, which may be used for the purpose of providing notice of the pendency of this action.

CLAIMS ALLEGED

COUNT I
[Negligence]

59. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs of this Complaint.

60. Home Depot owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, retaining, and safeguarding customers' personal financial information.

61. Home Depot owed a duty to Plaintiff and the Class to adequately protect its retail customers' personal and financial information.

62. Home Depot breached its duties by (1) unreasonably allowing an unauthorized third-party intrusion into its computer systems; (2) failing to reasonably protect against such an intrusion; (3) unreasonably allowing third parties to access the personal and private financial information of Home Depot customers; and (4) failing to appropriately monitor its systems to detect unauthorized access.

63. Home Depot knew or should have known the PCI DSS industry standard and other relevant requirements regarding cardholder data security, as well as the attendant risks of retaining personal and financial data and the importance of providing adequate security.

64. As a direct and proximate result of Home Depot's careless and negligent conduct, Plaintiff and the Class have suffered substantial financial losses as detailed herein.

65. These financial losses continue to grow as additional fraudulent charges to Home Depot customers are discovered.

COUNT II
[Negligence *Per Se*]

66. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs of this Complaint.

67. Under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Home Depot has a duty to protect and keep sensitive personal information that it obtained from cardholders that conducted debit and credit card transactions at Home Depot stores secure, private, and confidential.

68. Home Depot violated the Gramm-Leach-Bliley Act by: (1) failing to adequately protect its customers' sensitive personal and financial data; and (2) failing to monitor and ensure compliance with the PCI DSS, as well as its contractual obligations and accompanying rules and regulations.

69. Home Depot's violation of the PCI DSS, as well as its contractual obligations and accompanying rules and regulations, constitutes negligence *per se*.

70. As a direct and proximate result of Home Depot's negligence *per se*, Plaintiff and the Class have suffered substantial financial losses as detailed herein.

COUNT III
[Negligent Material Omission]

71. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs of this Complaint.

72. Home Depot, through its participation in the credit and debit card network, was required to comply with industry standards for card operation, including the PCI DSS. In order to comply with these standards, Home Depot was required to adequately protect cardholder personal and financial account data, to monitor access to that data, and not to retain, store, or disclose information obtained from card magnetic stripes beyond authorized boundaries.

73. Plaintiff and the Class reasonably relied on large, nationwide retail chains such as Home Depot to comply with PCI DSS and industry card operating regulations when Plaintiff and the Class issued debit and credit cards to customers and allowed them to be used at Home Depot stores.

74. Home Depot knew, or should have known, that it was not in compliance with PCI DSS and industry card operating regulations for protecting consumer data. Home Depot knew, or should have known, that it was not properly protecting cardholder personal and financial data.

75. Home Depot failed to communicate material information to Plaintiff and the Class regarding its non-compliance with PCI DSS and card operating regulations, including but not limited to the fact it was not properly safeguarding cardholder personal and financial account data.

76. Home Depot's failure to inform Plaintiff and Class members that it was not in compliance with PCI DSS and card operating regulations was a material omission, which it should have disclosed to Plaintiff and Class members.

77. Had Home Depot informed Plaintiff and Class members of its non-compliance with PCI DSS and industry regulations, Plaintiff and the Class would have been better able to protect themselves from the damages they have incurred and continue to incur.

78. As a direct and proximate result of Home Depot's negligent and improper conduct, Plaintiff and the Class have suffered substantial financial losses as detailed herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court enter judgment in its favor as follows:

A. Certifying the Class and appointing Plaintiff and its counsel to represent the Class;

B. Enjoining Home Depot from improperly retaining any personal or financial customer data;

C. Declaring that Home Depot is financially responsible for notifying all Class members about the defects described herein;

D. Awarding Plaintiff and the Class actual damages, consequential damages, specific performance, restitution, and/or rescission, where appropriate;

E. Awarding Plaintiff and the Class pre-judgment and post-judgment interest;

F. Awarding Plaintiff and the Class reasonable attorneys' fees and costs of suit; and

G. Awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims so triable.

Dated: November 10, 2014

Respectfully submitted,

W PITTS CARR & ASSOCIATES, PC

By: s/Pitts Carr
W. Pitts Carr (GA Bar # 112100)

Alex Weatherby (GA Bar # 819975)
10 North Parkway Square
4200 Northside Parkway
Atlanta, GA 30327
Tel: (404) 442-9000
Fax: (404) 442-9700
pcarr@wpcarr.com
aweatherby@wpcarr.com

Charles J. LaDuca
Daniel M. Cohen
CUNEO GILBERT & LADUCA, LLP
507 C Street NE
Washington, DC 20002
Tel: 202-789-3960
Fax: 202-789-1813

James J. Pizzirusso
Swathi Bojedla
HAUSFELD LLP
1700 K Street NW, Suite 650
Washington, DC 20006
Tel: (202) 540-7200
Fax: (202) 540-7201
jpizzirusso@hausfeldllp.com
sbojedla@hausfeldllp.com

Attorneys for Plaintiff and the Proposed Class