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

PHENIX-GIRARD BANK, 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 Phenix-Girard Bank ("Plaintiff" or "PGB"), individually and on behalf of similarly situated banks, credit unions, and other financial institutions (jointly "financial institutions"), files this Class Action Complaint against Defendant Home Depot U.S.A. Inc. ("Defendant" or "Home Depot"), and states the following:

INTRODUCTION

1. Plaintiff brings this 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' personally identifiable information ("PII") and private financial information.

2. On or around April 2014, computer hackers used malicious software in accessing point-of-sale ("POS") systems at Home Depot store locations throughout the U.S. and Canada. According to present reports, the hackers uploaded their malware on Home Depot's 7500 self-checkout machines. The hackers stole approximately 56 million 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. An additional 53 million customer email addresses were also stolen as later revealed by Home Depot.[1]

3. On or around September 2014, hackers listed the customers' stolen information for sale on the black-market website "rescator.cc." Hackers regularly sale stolen debit and credit card information on this website to other fraudsters who, in turn, wreak havoc on customers' lives through identity theft and draining their accounts. Meanwhile, financial institutions, such as Plaintiff, are left to sort through the immediate aftermath in attempting to monitor potential fraudulent transactions, close and reopen accounts, and reimburse their customers for fraudulent charges.

[1] Krebs on Security, "Home Depot: Hackers Stole 53M Email Addresses," available at: http://krebsonsecurity.com/tag/home-depot-breach/ (last accessed Dec. 10, 2014).

4. Home Depot's negligent security lapses enabled the theft of its customers' PII and financial information, as well as subsequent fraudulent charges on their debit and credit cards. Home Depot claims it was unaware of the massive 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 and restaurant chains including Target, Neiman Marcus, Sally Beauty, Harbor Freight Tools, and P.F. Chang's in months prior to the breach beginning at Home Depot. During this time, customers' PII and private financial information lay exposed to sale on the black market.

5. Home Depot waited to acknowledge their security breach *for nearly a week* and finally informed the public on September 8, 2014. The admission that a data breach had occurred was the first time that millions of customers' knew their PII and financial information was compromised to hackers.

6. Naturally, customers immediately began contacting Plaintiff regarding their compromised accounts and seeking Plaintiff and Class members' assistance in preventing further damages to related to identity theft, their financial accounts, and repercussions stemming from the loss of their PII and private financial information to hackers.

7. Home Depot's negligence and data security failures directly damaged the Plaintiff and the Class members. Plaintiff and Class members incurred significant damages in the hundreds of millions of dollars, including but not limited to: (a) reissuing debit and credit cards, loss of customers, (b) costs of reimbursing fraudulent charges, (c) notifying customers of the breach, (d) labor costs including overtime payments to employees and/or hiring temporary/part-time employees to respond to the breach, (e) reissuing checks, closing and opening new accounts, (f) lost interest and transaction fees, (g) lost opportunity costs, (h) increase fraud monitoring efforts and (g) handling an increase in customer service inquiries and investigations related to the breach. The Credit Union National Association ("CUNA") estimates that 7.2 million credit union cards were affected and credit unions incurred $60 million in direct costs. These figures do not include the full amount of damages represented by the different types of financial institutions represented by the Plaintiff and the Class. The damages are increased when one accounts for the direct costs and number of cards affected with other financial institutions, such as banks.

8. These costs are ongoing, as Plaintiff continues to investigate fraudulent transactions caused by the data breach that have not yet been reimbursed.

JURISDICTION AND VENUE

9. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The aggregated claims of the individual Class members exceed the sum or value of $5,000,000, exclusive of interests and costs and there are more than 100 Class members defined below, the majority of Class members are citizens of a different state than Defendant Home Depot.

10. 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, operates multiple stores across the state, 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.

11. Venue is proper in this District under 28 U.S.C. § 1391(a)(2) because, among other things, Home Depot's principal place of business is in Georgia and the unlawful conduct of Home Depot, out of which the causes of action arose, occurred in this District.

PARTIES

12. Plaintiff Phenix-Girard Bank is a chartered state chartered bank whose main offices are located in Phenix City, Alabama.

13. Plaintiff provides 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.

14. Defendant Home Depot U.S.A. Inc. 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 North America.

FACTUAL BACKGROUND

I. Security Parameters Failed to Comply with Industry Standards in Protecting Customers' PII and Private Financial Data.

15. Plaintiff and the Class members 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.

16. Retailers, including Home Depot, process credit and debit transactions through contracts with an acquiring bank. These contracts authorize and enable Home Depot the ability to process credit and debit transactions.

17. When a customer purchases a good, Home Depot requests authorization for the transaction from an issuer (such as Plaintiff, or any other Class member). When an issuer approves the transaction, Home Depot processes the transaction and forwards the purchase receipt to the acquiring bank it has contracted. Next, the acquiring bank pays Home Depot for the purchase and forwards 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.

18. Visa and MasterCard, among other payment-processing networks, issue 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: 1) cardholder account numbers, 2) personal information, 3) magnetic stripe information, or 4) transaction information to third parties other than the merchant's agent, the acquiring bank, or the acquiring bank's agents. The Card Operating Regulations requires Home Depot to maintain the security and confidentiality of debit and credit cardholder information and magnetic

stripe information and to protect this sensitive information and data from unauthorized disclosure to third-parties.

19. The April through September 2014 data breach at Home Depot demonstrates Home Depot's failing to comply with the Card Operating Regulations and a failure to inform Plaintiff and the Class of its non-compliance.

20. Home Depot is also bound 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. PCI DSS has twelve requirements:

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.[2]

21. On information and belief, PCI DSS compliance is required pursuant to Home Depot's contracts with acquiring banks. PCI DSS 2.0 was the standard in effect during the Home Depot data breach. Home Depot represented to Class members and the public that it met all current standards for PCI DSS.

22. PCI DSS compliance is not onerous and only represents minimal precautions that retailers should utilize to safeguard customer data at a baseline level.

[2] The PCI DSS 12 core security standards can be found here: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf, at pg. 5 (last accessed Dec. 9, 2014).

23. PCI DSS requires merchants, including 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 in its compliance with these standards.

24. PCI DSS requires Home Depot to protect its customers' PPI and private financial data and to prevent disclosure, or allow disclosure, any of this sensitive data to third parties.

25. Under the relevant PCI DSS standards, 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.

26. PCI DSS requires Home Depot consistent monitoring access to its computer networks and customer account data located on its systems. PCI DSS requires diligent monitoring precisely to ensure that data breaches are caught and quickly handled. PCI DSS standards require 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.

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

28. 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 and handles customers' accounts relied on Home Depot to adequately protect their PII and private financial data from unauthorized access.

29. 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.

II. Home Depot's Negligence Led to Financial Institution Customers' PII and Private Financial Data Hacked for Four Months.

30. Current reports reveal that Home Depot remained unaware of its security breach until receiving notification from law enforcement and from Class members. On its corporate website, Home Depot admits on September 2, 2014, it first became aware of a data breach involving the unauthorized access and theft of its customers' debit and credit card information.[3]

31. That same day, a substantial batch of debit and credit card data emerged for sale on "rescator.cc," a black market website known for marketing in stolen financial information. Rescator.cc is the website now infamous for selling customers' card information stolen in the Holiday 2013 Target data breach. Multiple Class members offered evidence that Home Depot stores as the likely source of the stolen data. Renowned security blogger Brian Krebs "broke" the story and posted evidence that the ZIP code data of the newly posted stolen data on rescator.cc and the ZIP code data of the Home Depot stores shared a 99.4 percent overlap.[4]

[3] *See* The Home Depot Provides Update on Breach Investigation, http://phx.corporate-ir.net/phoenix.zhtml?c=63646&p=RssLanding&cat=news&id=1964976 (last accessed Dec. 10, 2014).

[4] *See* Krebs on Security, Data: Nearly All U.S. Home Depot Stores Hit, available at: http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/ (last assessed Dec. 10, 2014).

32. 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.

33. Upon information and belief, Home Depot's security systems utilized 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.

34. After illicitly gaining access to Home Depot's networks, the hackers used "RAM scraper" malware to gain access to Home Depot customers' PII and private financial information. This malware is similar to the one used in the Target data breach.[5]

35. 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

[5] *See* Krebs on Secuirty, Home Depot Hit By Same Malware As Target, available at: http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/#more-27751 (last accessed Dec. 12, 2014).

malware, the type of malware installed on Home Depot's POS terminals, to harvest this unencrypted information.

36. Home Depot failed to detect the installation of RAM scraping malware on its POS terminals and failed to take steps to eliminate it.

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

38. 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.[6] The Alert instructs companies to:

a. "secure remote access connectivity,"

b. "implement secure network configuration, including egress and ingress filtering to only allow the ports/services necessary to conduct business" (i.e. segregate networks),

c. "actively monitor logs of network components, including intrusion detection systems and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses,"

[6] *See* Visa Data Security Alert, November 6, 2009, https://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf (last accessed Dec. 10, 2014).

d. "encrypt cardholder data anywhere it is being stored and… implement[] a data field encryption solution to directly address cardholder data in transit," and

e. "work with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration."

39. Additionally, Home Depot should have been aware of the U.S. Computer Emergency Readiness Team's alert to retailers regarding the dangers and threats posed by POS malware. The U.S. Computer Emergency Readiness Team, a unit within the Department of Homeland Security, released a guide on July 31, 2014 alerting retailers and Home Depot on how to protect their customers' PII and private financial information against the threat of POS malware attacks.[7]

40. The media reports that Home Depot's security breach could affect over 56 million credit and debit card accounts – nearly twenty million more than were

[7] US-CERT, Alert (TA14-212A) Backoff Point-of-Sale Malware, available at: https://www.us-cert.gov/ncas/alerts/TA14-212A (last accessed Dec. 12, 2012).

affected by the 2013 Target date breach.[8] Furthermore, the CUNA survey of credit unions found that damages could double those from the Target data breach.[9]

41. Home Depot never informed or warned Plaintiff and the Class about its deficient security systems and adherence to security protocols. Plaintiff and Class members reasonably expected that Home Depot would safeguard confidential customer PII and private financial information.

42. Indeed, security blogger Brian Krebs broke the news of the data breach to the public and Class members despite the breach occurring over a four month-long period. Home Depot failed to even report its own security breach and failures first.

III. Home Depot's Failure to Secure Customers' PII and Private Financial Information Damaged Plaintiff and Class Members.

43. Plaintiff and Class members 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

[8] *See* The Consumerist, Home Depot Hackers Used Self-Checkouts To Access 56M Credit/Debit Cards, 53M Email Addresses, available at: http://consumerist.com/2014/11/07/home-depot-hackers-used-self-checkouts-to-access-56m-creditdebit-cards-53m-email-addresses/ (last accessed Dec. 10, 2014).

[9] *See* CUNA, Home Depot breach cost CUs nearly double those from Target, available at: http://www.cuna.org/Stay-Informed/News-Now/Washington/Home-Depot-breach-cost-CUs-nearly-double-those-from-Target/ (last accessed Dec. 10, 2014).

customers, covering fraudulent transactions, and the expenses associated with monitoring and preventing further fraud due to the Home Depot security breach.

44. Home Depot failed to follow industry standards and did not effectively monitor its security systems to ensure the safety of customer information. Home Depot's substandard security protocols, improper retention of cardholder data, and failure to regularly monitor for unauthorized access caused the sensitive PII and financial data of Home Depot's customers to be compromised for weeks without warning to the Plaintiff or Class members.

45. Home Depot's security breach of systems was preventable. Several anonymous former Home Depot employees have described a work environment and culture involving "C-level security" (as opposed to A-level or B-level), which adversely impacted their IT security effectiveness.[10]

46. A July 2014 "health check" by Symantec on Home Depot's information systems revealed that Home Depot was using out-of-date malware detection systems. This was during the course of the data breach and hackers may have been accessing customers' PII and private financial data.

[10] *See* Ben Eglin, Michael Riley, & Dune Lawrence, Former Home Depot managers Depict 'C-Level' Security Before the Hack, BloombergBusinessweek, available at: http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say (last visited Dec. 10, 2014).

47. Three former Home Depot information security managers have stated that Home Depot was also using out-of-date antivirus software for its POS systems. Symantec released its Endpoint Protection Version 12 program in 2011, stating that the "threat landscape has changed significantly" and that Version 12 would protect against the "explosion in malware scope and complexity."[11]

48. 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.[12]

49. Home Depot admits it was bound by applicable security standards, including PCI DSS, and it was required to create and monitor a secure computer system that protects the PII and private financial data contained on customers' credit and debit cards. Home Depot 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.

50. Further, Home Depot had a duty to Plaintiff and the Class members to comply with card operating regulations, secure cardholder personal and financial

[11] *See* n. 10.
[12] *See id.*

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.

51. Home Depot breached these duties and negligently allowed sensitive cardholder data to be compromised throughout the April through September 2014 data breach.

52. 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.

53. 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.[13]

[13] BillGuard, Home Depot data breach likely to strike 60 million and cause over $2 billion in fraud, available at: http://blog.billguard.com/2014/09/home-depot-data-breach-estimated-impact/ (last accessed Dec. 12, 2014).

54. 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.[14]

CLASS ACTION ALLEGATIONS

55. 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[15] (the "Class").

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

57. The members of the Class are readily ascertainable.

[14] *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.").

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

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

59. 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.

60. 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.

61. 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.

62. 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.

63. 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

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

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

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

67. 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.

68. 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.

69. 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.

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

COUNT II
Negligence *Per Se*

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

72. 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.

73. 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.

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

75. 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 Misrepresentation By Omission

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

77. 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.

78. 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.

79. 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.

80. 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.

81. 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.

82. 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.

83. 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.

COUNT IV
Breach of Implied Contract

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

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

86. Home Depot breached the implied contracts it had made with Plaintiff and the Class by failing to safeguard such information.

87. The damages sustained by Plaintiff and the Class as described above were the direct and proximate result of Home Depot's breaches of these implied contracts.

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: December 12, 2014.

Respectfully submitted,

/s/ J. Benjamin Finley

J. BENJAMIN FINLEY
Georgia Bar Number 261504
MARYBETH V. GIBSON
Georgia Bar Number 725843
THE FINLEY FIRM, P.C.
Piedmont Center
3535 Piedmont Road
Bldg. 14, Ste. 230
Atlanta, GA 30305

JERE L. BEASLEY (BEA020)
Pro Hac Vice To Be Filed
W. DANIEL "DEE" MILES, III (MIL060)
Pro Hac Vice To Be Filed
LARRY A. GOLSTON (GOL029)
Pro Hac Vice To Be Filed
ANDREW E. BRASHIER (BRA156)
Pro Hac Vice To Be Filed
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

Attorneys for Plaintiff and Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on the 12th day of December, 2014, I have served a copy of the foregoing upon all parties below by e-file and/or by placing a copy of the same in the United States Mail, postage prepaid to the following:

Home Depot U.S.A. Inc.
c/o CSC of Cobb County, Inc.
192 Anderson Street, SE
Suite 125
Marietta, GA 30060

Pursuant to Local Rule 5.1, Northern District of Georgia, the foregoing is prepared in Times New Roman, 14 point font, double-spaced.

This 12th day of December, 2014.

/s/ J. Benjamin Finley

J. BENJAMIN FINLEY