IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF LOUISIANA

FIRST NBC BANK, **individually and on behalf** **of all others similarly situated,** **Plaintiff,** **v.** **HOME DEPOT, INC.** **Defendant.**	**CASE NUMBER:** **SECTION:** **DIVISION:**

CLASS ACTION COMPLAINT WITH JURY DEMAND

NOW INTO COURT, through undersigned counsel comes the Plaintiff, First NBC Bank, ("Plaintiff"), individually and on behalf of all others similarly situated, and upon personal knowledge of the facts pertaining to itself and on information and belief as to all other matters, to bring this Class Action Complaint against Home Depot, Inc. ("Home Depot" or the "Defendant") and allege as follows:

INTRODUCTION

1. Beginning some time in April of 2014 and continuing through September of 2014, personal and confidential credit and debit card information, including cardholder names, card numbers, expiration dates, security validation codes, and zip codes of approximately 56 million Home Depot customers was stolen by hackers (the "Security Breach").
2. The Security Breach was the direct and foreseeable result of Home Depot's failure to implement and maintain reasonable and industry-standard security measures to protect its customers' credit card, debit card, and personal information.

3. Yet, even though Home Depot failed to implement and maintain reasonable and industry-wide measures, it is this nation's financial institutions, including First NBC, that are left on the hook for tens, if not hundreds, of millions of dollars as a result of Home Depot's Security Breach.

4. Specifically, First NBC and other financial institutions suffered losses resulting from and relating to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest for transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer concerns and anxiety; and f) lost customers.

JURISDICTION AND VENUE

5. This Court has jurisdiction under 28 U.S.C. §1332(d) because: a) this matter was brought as a class action under Fed. R. Civ. P. 23; b) the class (as defined below) has more than 100 members; c) the amount at issue exceeds $5,000,000, exclusive of interest and costs; and d) at least one proposed Class member is a citizen of a state different from Home Depot.

6. This Court has personal jurisdiction over Home Depot because Home Depot transacts substantial business in this judicial district.

7. Venue is proper in this Court under 28 U.S.C. § 1391 (b)(2) and (c)(2), because, *inter alia*, Home Depot conducts substantial business in this district and is subject to personal jurisdiction in this district and damages to the Plaintiff occurred in this district.

PARTIES

8. The Plaintiff First NBC Bank is a Louisiana bank headquartered at 210 Baronne Street, New Orleans, Louisiana.

9. The Defendant Home Depot, Inc. is a Delaware corporation with its principal place of business located in Atlanta, Georgia.

FACTUAL ALLEGATIONS

I. Security breaches resulting in the disclosure of confidential information are becoming more common in the retail industry.

10. In the past year, the retail industry has had numerous data breaches similar to the Security Breach at Home Depot.

11. For example, between approximately November 27, 2013 and December 15, 2013, hackers infiltrated the network of Target Corporation and stole the credit card and debit card information of approximately 40 million Target customers.

12. In January of 2014, Michaels Stores, Inc., revealed that it experienced a data breach ultimately affecting 3 million of its customers.

13. In March of 2014, Sally Beauty Supply admitted to a data breach affecting at least 25,000 individuals.

14. In June of 2014, PF Chang's Chinese Bistro confirmed that 33 of its restaurant locations in the United States had data breaches and its customers' confidential information had been compromised.

II. The Home Depot Security Breach

15. Home Depot advertises and sells merchandise directly to millions of consumers through its retail stores in the United States.

16. In 2013, Home Depot reported annual sales of $78.8 billion.

17. Home Depot's U.S. retail stores use Point-of-Sale computer systems ("POS Systems"), which store credit card and debit card information.

18. When a customer makes a purchase at a Home Depot retail store using a credit card or debit card, Home Depot collects information relating to that card, including the card holder's name, account number, expiration date, card verification number, and personal identification number ("PIN") for ATM/debit cards.

19. Home Depot then stores this information in its POS System and transmits this information to a third party for completion of the payment.

20. Beginning in approximately April, 2014, hackers infiltrated Home Depot's POS Systems and network, and stole the credit card and debit card information of approximately 56 million Home Depot customers over a five month period.

21. This is the largest retail data breach ever.

22. Customer's names, credit and debit card numbers, card expiration dates, card verification values, and the ZIP codes of the stores associated with the transaction were compromised.

23. Upon information and belief, the hackers infiltrated Home Depot's POS Systems and computer network by installing malware that intercepted this data and then sent it back to the hackers.

24. According to published sources, Home Depot's Security Breach involved substantially similar malware used by hackers in the Target data breach.[1]

[1] *See, e.g.,* Krebs on Security, Home Depot Hit by Same Malware as Target, September 7, 2014, *available at* http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/#more-27751 (last accessed on September 21, 2014).

25. Home Depot knew or should have known that data breaches were endemic throughout the retail industry.

26. Despite this knowledge of data breaches 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.

27. Additionally, Home Depot failed to detect this breach for more than four months.

28. It was only after law enforcement and financial institutions told Home Depot of unusual activity on cards used at Home Depot retail stores that it finally became aware of the breach.

III. Home Depot is internally unaware of attacks on its system.

29. 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]

30. Home Depot responded that it was "looking into some unusual activity," but would not confirm that a breach occurred.[3]

31. It was not until September 8, 2014 that Home Depot confirmed the breach and revealed that it could impact 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.[4]

---

[2] *See* Krebs on Security, Banks: Credit Card Breach at Home Depot, September 2, 2014, *available at* http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/#more-27671 (last accessed on September 21, 2014).
[3] *Id.*
[4] *See* The Home Depot Provides Update on Breach Investigation, September 8, 2014 News Release, *available at* http://phx.corporate-ir net/phoenix.zhtml?c=63646&p=irol-newsArticle&ID=1964976&highlight= (last accessed on September 21, 2014)

32. 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.[5]

IV. Home Depot failed to maintain reasonable and industry-standard security measures in spite of the prior data breaches.

33. The Security Breach occurred as a result of Home Depot's failure to implement reasonable and industry-standard security measures.

34. There are several parties to a typical credit or debit card transaction. The transaction begins when a cardholder uses a debit card or credit card at the point-of-sale system of a merchant (in this case Home Depot). The point-of-sale system then transmits the card information (data encoded on the magnetic strip) first to the checkout register and then to an acquiring bank, which the merchant contracts with to process the merchant's debit card and credit card transactions.

35. The acquiring bank then transmits the card information and a request message to a processor, generally, the card company, such as Visa, MasterCard, or American Express. The processor then routes the request to an issuing bank for review and approval.

36. The issuing bank is the financial institution that issued the credit or debit card directly to the consumer. The Plaintiff and the other Class Members are issuing banks. If the transaction is approved, the issuing bank will post the transaction to the consumer's credit card or debit card account.

37. Credit card companies require merchants, such as Home Depot, to comply with certain regulations aimed at safeguarding customer information.

38. In 2006, Visa, MasterCard, and other members of the payment card industry ("PCI")

[5] *Id.*

established the Security Standards Council ("PCI SSC"). The PCI SSC establishes Payment Card Industry Data Security Standards ("PCI DSS") and Payment Application Data Security Standards ("PA-DSS"), which are a set of requirements designed to ensure that all companies, including merchants such as Home Depot, that process, store, or transmit credit card and debit card information maintain a secure environment.

39. The twelve baseline requirements are:

- **Build and Maintain a Secure Network and Systems**
    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 and Security Policy**

12. Maintain a policy that addresses information security for all personnel.[6]

40. Home Depot was at all times fully aware of its data protection obligations resulting 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 that must be protected.

41. As a result of its participation in the payment card processing networks, Home Depot was obligated to fully comply with the PCI DSS and other PCI requirements relating to the security of customer credit card and debit card information.

42. Home Depot knew or should have known that 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.

43. Home Depot also knew or should have known that if it failed to secure its customers' sensitive financial information, the financial institutions issuing the payment cards to its customers, *i.e.*, the Plaintiff and the Class, would suffer harm relating to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest for transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with

[6] *See* Payment Card Industry, Data Security Standard, Requirements and Security Assessment Procedures, v.3.0, November, 2013, *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf (last accessed September 21, 2014).

monitoring and preventing fraud; e) administrative expenses in responding to customer concerns and anxiety; and f) lost customers.

44. Despite this knowledge, Home Depot's treatment of its customer's data fell woefully short of its duties and obligations.

45. At the time of the Security Breach the Home Depot should have had specific notice of the potential for a Security Breach in its internal system but did not take sufficient precautions in spite of this knowledge.

46. It was only after the Security Breach that Home Depot "completed a major payment security project that provides enhanced encryption of payment data at point of sale in the company's U.S. stores, offering significant new protection for customers."[7]

47. Reports in the media have described Home Depot's IT security department as content with "C-level security."[8]

48. A Bloomberg Businessweek report, relying on interviews with former Home Depot employees, identified the following problems with Home Depot's approach to IT security: a) Home Depot's payment systems were not configured to properly encrypt customer payment card data; b) Home Depot's IT department experienced high employee turnover; c) Home Depot was using outdated malware detection programs, including a seven-year-old Symantec program, Endpoint Protection 11; d) 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

[7] *See* The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores, September 18, 2014 Press Release, *available at* http://media.corporate-ir.net/media_files/IROL/63/63646/HD_Data_Update_II_9-18-14.pdf (last accessed September 21, 2014).

[8] Former Home Depot Managers Depict 'C-Level' Security Before the Hack, BloombergBusinessweek, Ben Elgin, Michael Riley, and Dune Lawrence, September 12, 2014, *available at* http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say, last accessed on September 21, 2014.

announced it would end all support for it by January 2015; and e) 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.[9]

49. Other interviews with former employees revealed that Home Depot did not regularly scan the computer systems for vulnerabilities inside its retail stores and "more than a dozen systems handling customer information were not assessed and were off limits to much of the security staff."[10]

50. When employees requested new security software or training, "managers came back with the same response: 'We sell hammers.'"[11]

V. Financial Institutions Have Been Harmed by Home Depot's Failure to Implement Reasonable and Industry-Standard Security Measures

51. Financial institutions, including the Plaintiff and other Class Members, have suffered losses resulting from the Security Breach relating to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest in transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer confusion; and f) lost customers.

---

[9] *Id.*

[10] Ex-Employees Say Home Depot Left Data Vulnerable, The New York Times, Julie Creswell and Nicole Perlroth, September 19, 2014, *available at* http://www nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?_r=0 (last accessed September 22, 2014).

[11] *Id.*

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

53. Indeed, Home Depot's public statements to customers after the data breach state Home Depot's belief that card-issuing institutions are responsible for fraudulent charges on cardholder accounts resulting from the Security Breach.[12]

54. Home Depot, at all times relevant to this action, had a duty to, and represented to the Plaintiff and members of the Class that it would: a) properly secure payment card magnetic stripe information at the point of sale and on Home Depot's internal networks; b) encrypt payment card data using industry standard methods; c) use available technology to defend its POS Systems from well-known methods of attack; and d) act reasonably to prevent the foreseeable harms to the Plaintiff and the Class which would naturally result from payment card data theft.

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

56. As a result of the events detailed herein, the 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.

---

[12] *See* Frequently Asked Questions, *available at*, https://corporate homedepot.com/MediaCenter/Documents/FAQs.pdf (last accessed on September 21, 2014 (contending that "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.").

57. As a result of the Security Breach, in order to protect its customers and avoid fraud losses, First NBC reissued and mailed replacement cards to affected customers.

58. First NBC has also incurred losses as a result of the Security Breach from lost interest in transaction fees, including lost interchange fees; incurring administrative expenses and overhead charges associated with monitoring and preventing fraud and responding to customer confusion; and lost customers.

59. On information and belief Class Members have also incurred losses as a result of the Security Breach on account of reimbursing customers for fraudulent charges, as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205

60. Numerous other Class Members issued and sent replacement cards as a result of the Security Breach.

61. Replacing a credit card or debit card can cost a financial institution as much or more than $10 to $12 per card.

CLASS ACTION ALLEGATIONS

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

> All banks, credit unions, and other financial institutions in the United States, including its territories and protectorates, 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 through September 18, 2014 ("the Class").

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

64. This action is brought and may properly be maintained as a class action pursuant to 28 U.S.C. § 1332(d). This action satisfies the procedural requirements set forth in Fed. R. Civ. P. 23.

65. There are substantial questions of law and fact common to the Class. The questions include, but are not limited to, the following:

    a. Whether Home Depot failed to employ reasonable and industry-standard measures to secure and safeguard its customers' credit card, debit card and personal information;

    b. Whether Home Depot properly implemented and maintained its purported security measures to protect its customers' credit card, debit card and personal information;

    c. Whether Home Depot misrepresented that it did not retain customer financial information and misrepresented that its customers' financial and personal information was secure;

    d. Whether Home Depot's security failures resulted in harm to Home Depot's customers' financial and personal information being accessed and disseminated by thieves;

    e. Whether Home Depot was negligent in failing to properly secure and protect its customers' financial and personal information;

    f. Whether the Plaintiff and other members of the Class are entitled to injunctive relief; and

    g. Whether the Plaintiff and other members of the Class are entitled to damages and the measure of such damages.

66. The Plaintiff's claims are typical of the claims of the Class Members. Plaintiff and all Class Members were damaged by the same unreasonable conduct of Home Depot.

67. The Plaintiff will fairly and adequately protect and represent the interests of the Class. The interests of the Plaintiff coincide with, and are not antagonistic to, those of the Class.

68. The Plaintiff has retained counsel competent and experienced in complex class action litigation.

69. Members of the Class are so numerous that joinder is impracticable. The Plaintiff believes that there are hundreds, if not thousands, of Class Members.

70. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual Class Members, because Home Depot has acted on grounds generally applicable to the entire Class. Thus, determining damages with respect to the Class as a whole is appropriate.

71. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated entities to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender.

72. The Plaintiff knows of no special difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

COUNT ONE
Negligence

73. The Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

74. Home Depot had an affirmative duty to exercise reasonable care in safeguarding and protecting its customers' financial and personal information, including credit card and debit card information.

75. Home Depot violated its duty by: a) allowing a third-party intrusion into its computer systems; b) failing to protect against such an intrusion; c) failing to detect the intrusion for a period of four or more months; and d) allowing the personal and financial information of customers of the Plaintiff and the Class to be accessed by third parties on a massive scale.

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

77. Home Depot knew or should have known that its failure to take reasonable measures to protect its POS Systems against obvious risks would result in harm to the Plaintiff and the Class.

78. It was foreseeable that Home Depot's failure to exercise reasonable care in protecting its customers' credit card, debit card, and personal information would result in the Plaintiff and the other Class Members suffering losses related to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest in transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer confusion; and f) lost customers.

79. It was foreseeable that Home Depot's failure to take reasonable measures to protect its POS Systems against obvious risks would result in the Plaintiff and the other Class Members

suffering losses related to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest in transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer confusion; and f) lost customers.

80. As a direct result of Home Depot's failure to secure and protect its customers' credit card, debit card, and personal information, Plaintiff and the other Class Members were damaged by losses related to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest in transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer confusion; and f) lost customers.

81. As a direct result of Home Depot's failure to take reasonable measures to protect its POS Systems, the Plaintiff and the other Class Members were damaged by losses related to: a) the expense of creating, issuing, and mailing new payment cards to their customers; b) customer reimbursements for fraudulent charges as required by the Electronic Transfers Act, 15 U.S.C. § 1693, and 12 C.F.R. §205; c) lost interest in transaction fees, including lost interchange fees; d) administrative expenses and overhead charges associated with monitoring and preventing fraud; e) administrative expenses in responding to customer confusion; and f) lost customers.

82. Home Depot's wrongful actions and/or inaction (as described above) constituted negligence at common law and under civilian law.

COUNT TWO
Negligent Misrepresentation

83. The Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

84. Millions of Home Depot's customers made purchases at Home Depot stores with credit cards and debit cards issued by Plaintiff and the other Class Members.

85. Home Depot represented to the Plaintiff and the Plaintiff's customers that it would safeguard and protect its customers' financial and personal information from harm. Credit Card Operating Rules and PCI standards provide reasonable commercial standards for safeguarding and protecting customer credit card and debit card information from harm.

86. Home Depot's promises to safeguard and protect its customers' financial and personal information were material facts upon which the Plaintiff and other Class Members relied.

87. Home Depot was not in compliance with one or more Credit Card Operating Rules and PCI Standards at the time of the Security Breach, and was not properly safeguarding customer data.

88. The Plaintiff and the other Class Members reasonably relied on Home Depot to comply with the Credit Card Operating Rules and PCI standards, and Home Depot's representations that it would safeguard customer data.

89. Had the Plaintiff and the Class known that Home Depot was not compliant with the Card Operating Regulations and the PCI DSS, the 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.

90. The Plaintiff and the other Class Members suffered actual damages as a result of Home Depot's negligent misrepresentations.

COUNT FOUR
Negligent Performance of Services

91. The Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

92. Home Depot had a pecuniary interest in processing its customers' credit card and debit card transactions.

93. In addition to its pecuniary interests, Home Depot processed its customers' credit card and debit card transactions for the benefit of assigning banks, credit card companies, and issuing banks—including the Plaintiff and the other Class Members—which also had a pecuniary interest in such transactions.

94. The Plaintiff and the other Class Members relied upon Home Depot to exercise reasonable care in processing credit card and debit card transactions and to ensure that sensitive credit card and debit card information remained secure.

95. Home Depot failed to exercise reasonable care in processing credit card and debit card transactions by failing to implement reasonable and industry-standard security measures.

96. The Plaintiff and the other Class members suffered actual damages as a result of Home Depot's failure to exercise reasonable care in processing credit card and debit card transactions.

JURY TRIAL DEMAND

97. The Plaintiff, individually and on behalf of all others similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on all claims so triable.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiff, individually and on behalf of the Class, respectfully requests that the Court:

A. Determine that this action may be maintained as a class action pursuant to Federal Rule of Civil Procedure 23(a), (b)(2) and (b)(3);

B. Direct that reasonable notice of this action, as provided by Federal Rule of Civil Procedure 23(c)(2), be given to the Class;

C. Appoint the Plaintiff as Class Representative;

D. Appoint the Plaintiff's counsel as Class Counsel;

E. Enter judgment against Home Depot and in favor of the Plaintiff and the Class;

F. Adjudge and decree under Fed. R. Civ. P. 57 and 18 U.S.C. § 2201(a) that the acts alleged herein by Home Depot constitute negligence, negligent misrepresentations, and negligent performance of services;

G. Award all compensatory and statutory damages to the Plaintiff and the Class in an amount to be determined at trial;

H. Award punitive damages, including treble and/or exemplary damages, in an appropriate amount;

I. Enter an injunction permanently barring continuation of the conduct complained of herein, and mandating Home Depot be required to adopt and implement appropriate systems, controls, policies and procedures to ensure Home Depot remains in compliance with duties required by law and industry standards, and further mandating that Home Depot install such systems, controls, policies and procedures implemented to achieve full remuneration and relief to the Plaintiff and the Class;

J. Award the Plaintiff and the Class the costs incurred in this action together with reasonable attorneys' fees and expenses, including any necessary expert fees as well as pre-judgment and post-judgment interest; and

K. Grant such other and further relief as is necessary to correct for the effects of Home Depot's unlawful conduct and as the Court deems just and proper.

DATED: September 22, 2014

Respectfully submitted,

/s/Korey A. Nelson
Stephen B. Murray, Sr. (9858)
Stephen B. Murray, Jr. (23877)
Arthur M. Murray (27694)
Korey A. Nelson (30002)
MURRAY LAW FIRM
650 Poydras Street
Suite 2150
New Orleans, Louisiana 70130
Tel: 504.525.8100
Fax: 504.584.5249
smurray@murray-lawfirm.com
smurrayjr@murray-lawfirm.com
amurray@murray-lawfirm.com
knelson@murray-lawfirm.com

Counsel for the Plaintiff and Proposed Class