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

In re: The Home Depot, Inc. Customer Data Breach Litigation	)	**MDL No. 14-02583-TWT**
This Document Relates to: All Financial Institution Cases	)	**CONSOLIDATED CLASS ACTION COMPLAINT**
	)	**JURY TRIAL DEMANDED**

FINANCIAL INSTITUTION PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT

"If we rewind the tape, our security systems could have been better…Data security just wasn't high enough in our mission statement."

Frank Blake, Home Depot's recently retired Chief Executive Officer and Current Chairman of the Board

TABLE OF CONTENTS

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiff Financial Institutions (identified below) individually and on behalf of similarly situated banks, credit unions, and other financial institutions, and the Association Plaintiffs (identified below) acting on behalf of their members, file this Consolidated Class Action Complaint against Defendants, The Home Depot, Inc. and Home Depot U.S.A. Inc. (collectively "Defendants" or "Home Depot"), and allege the following based upon personal knowledge with respect to Plaintiffs and otherwise on information and belief derived from, among other things, investigation of counsel and review of public documents:

INTRODUCTION

1. Between April, 2014 and September, 2014, Home Depot was subject to one of the largest retail data breaches in our nation's history. Taking advantage of substantial weaknesses and vulnerabilities in the company's data security systems, hackers stole the personal and financial information of approximately 56 million Home Depot customers across the country. The stolen information was then sold on the internet to thieves who made massive numbers of fraudulent transactions on credit and debit cards issued to Home Depot customers.

2. The data breach was the inevitable result of Home Depot's longstanding approach to the security of its customer's confidential data, an

approach characterized by neglect, incompetence, and an overarching desire to minimize costs. For years before the breach, notwithstanding the pleas of its own employees, Home Depot refused to upgrade critical security systems; ignored experts' warnings about the vulnerability of its computer network; placed ineffective leadership in key information technology positions; and disregarded applicable industry standards. Indeed, in March, 2015, an independent investigator employed by the payment card networks determined that Home Depot was not in compliance with industry standards at the time of the breach.

3. Home Depot's data security deficiencies were so significant that, even after hackers entered its systems, their activities went undetected for approximately five months, despite red flags that should have caused Home Depot to discover their presence and thwart, or at least, limit the damage. Home Depot learned of the breach only after being notified by the U.S. Secret Service and the breach had been publicized by a prominent security blogger.

4. The financial costs caused by Home Depot's misconduct have been borne in large part by the institutions that issued the payment cards compromised by the breach. These costs include, but are not limited to, canceling and reissuing millions of compromised cards and reimbursing their customers for fraudulent charges. Industry sources estimate that community banks and credit unions –

which together issued only a fraction of the compromised cards – incurred more than $150 million in reissuance costs alone. Industry sources further estimate that the total fraud losses for all financial institutions are in the billions of dollars.

5. This class action is brought by the Financial Institution Plaintiffs – banks and credit unions located in forty-four states and the District of Columbia with collective assets of about $115 billion – to recover the costs that they and others similarly situated have been forced to bear as a direct result of the Home Depot data breach and to obtain other equitable relief. Plaintiffs assert claims for negligence and negligence *per se* on behalf of a national class, or, alternatively, if a national class is not certified, on behalf of statewide classes in the states in which named plaintiffs are located. In addition, claims are asserted for violation of various state statutes on behalf of eight state subclasses.

6. The Credit Union National Association and sixteen state credit union associations and leagues, whose members were damaged by the Home Depot data breach, also join this action as plaintiffs. These entities, referred to in this complaint as the Association Plaintiffs, are not seeking damages, but rather equitable relief on behalf of their members. The credit unions belonging to the Association Plaintiffs are owned by more than 100 million Americans.

JURISDICTION AND VENUE

7. This Consolidated Class Action Complaint supersedes all other complaints in actions filed by financial institutions that were consolidated in this multi-district proceeding and is subject to the same rules and jurisdictional requirements as any other action originally filed in this judicial district.

8. 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 interest and costs; there are more than 100 putative class members defined below; and minimal diversity exists because the majority of putative class members are citizens of a different state than Defendants.

9. This Court has personal jurisdiction over Defendants because each Defendant maintains its principal headquarters in Georgia, is registered to conduct business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendants intentionally avail themselves of this jurisdiction by conducting their corporate operations here and promoting, selling, marketing, and distributing Home Depot products to Georgia residents.

10. Venue is proper in this District under 28 U.S.C. § 1391(a)(2) because, among other things, Defendants' principal places of business are in Georgia, and a

substantial part of the events, acts, and omissions giving rise to the claims of the Plaintiffs occurred in this District.

PARTIES

Financial Institution Plaintiffs

11. The Financial Institution Plaintiffs -- listed below in order of the state in which they are located -- issued and owned payment cards compromised by the Home Depot data breach and suffered resulting injuries, including but not limited to the cost of reissuing cards and fraud losses:

12. Plaintiff Army Aviation Center Federal Credit Union ("Army Aviation") is a federally chartered credit union with assets of approximately $1.1 billion. Army Aviation is headquartered in Alabama and has branches in Alabama and Florida.

13. Plaintiff Denali Alaskan Federal Credit Union ("Denali") is a federally chartered credit union with assets of approximately $571 million. Denali is headquartered in Alaska and has branches in Alaska and Washington.

14. Plaintiff Alcoa Community Federal Credit Union ("Alcoa Community") is a federally chartered credit union. Alcoa Community is headquartered in Arkansas and has branches only in Arkansas.

15. Plaintiff Coasthills Credit Union ("Coasthills") is a California

chartered credit union with assets of approximately $740 million. Coasthills is headquartered in California and has branches only in California.

16. Plaintiff Redwood Credit Union ("Redwood") is a California chartered credit union with assets of approximately $2.6 billion. Redwood is headquartered in California and has branches only in California.

17. Plaintiff Aventa Credit Union ("Aventa") is a Colorado chartered credit union with assets of approximately $158 million. Aventa is headquartered in Colorado and has branches only in Colorado.

18. Plaintiff Savings Institute Bank & Trust ("Savings Institute") is a Connecticut chartered bank with assets of approximately $1.5 billion. Savings Institute is headquartered in Connecticut and has branches in Connecticut and Rhode Island.

19. Plaintiff Delaware Alliance Federal Credit Union ("DAFCU") is a federally chartered credit union with assets of approximately $20 million. DAFCU is headquartered in Delaware and has its sole branch in Delaware.

20. Plaintiff Democracy Federal Credit Union ("Democracy FCU") is a federally chartered credit union based in the District of Columbia with assets of approximately $152 million. Democracy FCU is headquartered in Virginia and has branches in Virginia, the District of Columbia, Maryland, and Pennsylvania.

21. Plaintiff Suncoast Credit Union ("Suncoast") is a Florida chartered credit union with assets of approximately $5.9 billion. Suncoast is headquartered in Florida and has branches only in Florida.

22. Plaintiff Atlanta Postal Credit Union ("Atlanta Postal") is a Georgia chartered credit union with assets of approximately $2 billion. Atlanta Postal is headquartered in Georgia and has branches in Georgia and North Carolina.

23. Plaintiff Georgia's Own Credit Union ("Georgia's Own") is a Georgia chartered credit union with assets of approximately $1.8 billion. Georgia's Own is headquartered in Georgia and has branches only in Georgia.

24. Plaintiff Big Island Federal Credit Union ("Big Island") is a federally chartered credit union with assets of approximately $81 million. Big Island is headquartered in Hawaii and has branches only in Hawaii.

25. Plaintiff Idaho Central Credit Union ("Idaho Central") is an Idaho chartered credit union with assets of approximately $2 billion. Idaho Central is headquartered in Idaho and has branches only in Idaho.

26. Plaintiff University of Illinois Employees Credit Union ("UIECU") is an Illinois chartered credit union with assets of approximately $294 million. UIECU is headquartered in Illinois. All UIECU branches are located in Illinois.

27. Plaintiff Elements Financial Federal Credit Union f/k/a Eli Lilly

Federal Credit Union ("Elements Financial") is a federally chartered credit union with assets of approximately $1 billion. Elements Financial is headquartered in Indiana and has branches only in Indiana.

28. Plaintiff First Gateway Credit Union ("First Gateway") is an Iowa chartered credit union with assets of approximately $95 million. First Gateway is headquartered in Iowa and has branches in Iowa and Illinois.

29. Plaintiff Credit Union of America ("Credit Union of America") is a Kansas chartered credit union with assets of approximately $596 million. Credit Union of America is headquartered in Kansas and has branches only in Kansas.

30. Plaintiff First NBC Bank ("First NBC") is a Louisiana chartered bank with assets of approximately $3.7 billion. First NBC is headquartered in Louisiana and has branches only in Louisiana.

31. Plaintiff Maine Highlands Federal Credit Union ("Maine Highlands") is a federally chartered credit union with assets of approximately $95 million. Maine Highlands is headquartered in Maine and has branches only in Maine.

32. Plaintiff State Employees Credit Union of Maryland ("SECU") is a Maryland chartered credit union with assets of approximately $2.9 billion. SECU is headquartered in Maryland and has branches only in Maryland.

33. Plaintiff Pittsfield Cooperative Bank ("Pittsfield Cooperative") is a

Massachusetts chartered bank with assets of approximately $254 million. Pittsfield Cooperative is headquartered in Massachusetts and has branches only in Massachusetts.

34. Plaintiff Charlevoix State Bank ("Charlevoix") is a Michigan chartered bank with assets of approximately $158 million. Charlevoix is headquartered in Michigan and has branches only in Michigan.

35. Plaintiff Profinium Financial, Inc. ("Profinium") is a Minnesota chartered bank with assets of approximately $323 million. Profinium is headquartered in Minnesota and has branches only in Minnesota.

36. Plaintiff Navigator Credit Union ("Navigator") is a Mississippi chartered credit union with assets of approximately $289 million. Navigator is headquartered in Mississippi and has branches in both Mississippi and Alabama.

37. Plaintiff K.C. Police Credit Union ("KCPCU") is a Missouri chartered credit union with assets of approximately $112 million. KCPCU is headquartered in Missouri and has branches only in Missouri.

38. Plaintiff Valley Federal Credit Union ("Valley Federal") is a federally chartered credit union with assets of approximately $211 million. Valley Federal is headquartered in Montana and has branches in Montana and Wyoming.

39. Plaintiff Financial Horizons Credit Union ("Financial Horizons") is a

Nevada chartered credit union with assets of approximately $155 million. Financial Horizons is headquartered in Nevada and has branches only in Nevada.

40. Plaintiff Bellwether Community Credit Union ("Bellwether") is a New Hampshire chartered credit union with assets of approximately $408 million. Bellwether is headquartered in New Hampshire and has branches only in New Hampshire.

41. Plaintiff Hudson City Savings Bank ("Hudson City") is a New Jersey chartered bank with assets of approximately $36 billion. Hudson City is headquartered in New Jersey and has branches in Connecticut, New Jersey, and New York.

42. Plaintiff First Financial Credit Union ("First Financial") is a New Mexico state chartered credit union with assets of approximately $427 million. First Financial is headquartered in New Mexico and has branches only in New Mexico.

43. Plaintiff Amalgamated Bank ("Amalgamated") is a New York chartered bank with assets of approximately $3.8 billion. Amalgamated is headquartered in New York City and has branches in New York, New Jersey, California, and Washington D.C.

44. Plaintiff High Point Bank ("High Point") is a North Carolina chartered

bank with assets of approximately $828 million. High Point is headquartered in North Carolina and has branches only in North Carolina.

45. Plaintiff Greater Cincinnati Credit Union ("GCCU") is an Ohio chartered credit union with assets of approximately $88 million. GCCU is headquartered in Ohio and has branches only in Ohio.

46. Plaintiff WEOKIE Credit Union ("WEOKIE") is an Oklahoma chartered credit union with assets of approximately $1 billion. WEOKIE is headquartered in Oklahoma and has branches only in Oklahoma.

47. Plaintiff Oregon Community Credit Union ("Oregon Community") is an Oregon chartered credit union with assets of approximately $1.2 billion. Oregon Community is headquartered in Oregon and has branches only in Oregon.

48. Plaintiff American Heritage Federal Credit Union ("American Heritage") is a federally chartered credit union with assets of approximately $1.5 billion. American Heritage is headquartered in Pennsylvania and has branches in Pennsylvania and New Jersey.

49. Plaintiff First Columbia Bank and Trust Company ("First Columbia") is a Pennsylvania chartered bank with assets of approximately $636 million. First Columbia is headquartered in Pennsylvania and has branches only in Pennsylvania.

50. Plaintiff Navigant Credit Union ("Navigant") is a Rhode Island state

chartered credit union with assets of approximately $1.5 billion. Navigant is headquartered in Rhode Island and has branches only in Rhode Island.

51. Plaintiff Greenville Heritage Federal Credit Union ("Greenville Heritage") is a federally chartered credit union with assets of approximately $78 million. Greenville Heritage is headquartered in South Carolina and has branches only in South Carolina.

52. Plaintiff Electric Service Credit Union ("Electric Service") is a Tennessee chartered credit union with assets of approximately $54 million. Electric Service is headquartered in Tennessee and has branches only in Tennessee.

53. Plaintiff American Airlines Federal Credit Union ("American Airlines FCU") is a federally chartered credit union with assets of approximately $5.6 billion. American Airlines FCU is headquartered in Texas and has branches in Arizona, California, Florida, Illinois, Massachusetts, Missouri, New York, New Jersey, North Carolina, Oklahoma, Pennsylvania, Tennessee, Texas, and Virginia.

54. Plaintiff American Bank of Commerce ("American Commerce") is a Texas chartered bank with assets of approximately $691 million. American Commerce is headquartered in Texas and has branches in Colorado and Texas.

55. Plaintiff Deseret First Federal Credit Union ("Deseret First") is a

federally chartered credit union with assets of approximately $461 million. Deseret First is headquartered in Utah and has branches only in Utah.

56. Plaintiff Pentagon Federal Credit Union ("Pentagon FCU") is a federally chartered credit union with assets of approximately $18.5 billion. Pentagon FCU is headquartered in Virginia and has branches in Florida, Hawaii, Maryland, New York, North Carolina, Tennessee, Texas, Virginia, and Washington D.C.

57. Plaintiff United Bank (VA) ("United Bank Virginia") is a Virginia chartered bank with assets of approximately $7.3 billion. United Bank Virginia is headquartered in Virginia and has branches in Maryland, Ohio, Pennsylvania, Virginia, Washington D.C., and West Virginia.

58. Plaintiff Sound Community Bank ("Sound Community") is a Washington chartered bank with assets of approximately $495 million. Sound Community is headquartered in Washington and has branches only in Washington.

59. Plaintiff United Bank (WV) ("United Bank West Virginia") is a West Virginia chartered bank with approximately $5.4 billion. United Bank West Virginia is headquartered in West Virginia and has branches in Maryland, Ohio, Pennsylvania, Virginia, Washington D.C., and West Virginia.

60. Plaintiff Firefighters Credit Union ("Firefighters CU") is a Wisconsin

chartered credit union with assets of approximately $64 million. Firefighters CU is headquartered in Wisconsin and has branches only in Wisconsin.

61. Plaintiff Atlantic City Federal Credit Union ("Atlantic City") is a federally chartered credit union with assets of approximately $112 million. Atlantic City is headquartered in Wyoming and has branches only in Wyoming.

Association Plaintiffs

62. The Association Plaintiffs are associations whose members were damaged as a result of the Home Depot data breach and likely will suffer further damage if another data breach occurs. The Association Plaintiffs are non-class plaintiffs. While the Association Plaintiffs have themselves been injured by the Home Depot data breach, they do not seek money damages. Rather, the Association Plaintiffs bring this action for equitable relief on behalf of their members and have standing to do so because their members would otherwise have standing to sue in their own right; the interests they seek to protect are germane to their respective purposes; and the relief sought does not require participation of individual members. The Association Plaintiffs are as follows:

63. Plaintiff Credit Union National Association ("CUNA"), headquartered in Washington, D.C., is the largest association of credit unions in the United States. Credit unions are not-for-profit cooperatives providing financial services to people

from all walks of life and are owned by the consumers that the credit unions serve. CUNA represents more than 5,000 credit unions, which are owned by more than 100 million consumer members throughout the United States. CUNA's purpose includes representing and serving the interests of its members by, among other things, organizing and focusing their advocacy efforts; providing education and training; and serving as a forum for its members to meet and share ideas regarding their operations and industry.

64. Plaintiff California and Nevada Credit Union League ("California and Nevada CUL") is the largest state-wide association of credit unions in the United States. California and Nevada CUL is headquartered in California and has 307 member credit unions, which have more than $125 billion in assets and are owned by more than nine million consumers throughout California and Nevada. California and Nevada CUL's purpose includes ensuring the sustained health of its members and helping credit unions change people's lives.

65. Plaintiff Georgia Credit Union League ("Georgia CUL") is an association of credit unions with its headquarters in Georgia. Georgia CUL represents 133 credit unions with combined assets of more than $19 billion. Georgia CUL's purpose includes advocating for its members and assisting its members to become the premier source of financial services for Georgians.

66. Plaintiff Illinois Credit Union League ("Illinois CUL") is an association of credit unions headquartered in Illinois. Illinois CUL's members collectively have over $35 billion in assets and are owned by nearly three million members. Illinois CUL's purpose includes advocating on behalf of its members and providing its members with a favorable operating environment, quality information, and products and services enabling them to exist, compete and prosper in the financial marketplace.

67. Plaintiff Indiana Credit Union League ("Indiana CUL") is an association of credit unions headquartered in Indiana. Indiana CUL has over 170 member credit unions, which have approximately $21.5 billion in assets and are owned by more than two million consumers throughout Indiana. Indiana CUL's purpose is to help credit unions through advocacy to protect and further their its members' interests, by offering consultation, legislative, and regulatory support, and by providing public relations, operational and technical assistance, education, and training.

68. Plaintiff Maine Credit Union League ("Maine CUL") is an association headquartered in Maine with 60 credit union members. Maine CUL's members collectively have over $6 billion in assets and are owned by over 650,000 consumers. Maine CUL's purpose includes advocating on behalf of its members

and promoting the growth and financial health of credit unions through delivery of quality products and services.

69. Plaintiff Montana Credit Union Network ("Montana CUN") is an association of credit unions headquartered in Montana. Montana CUN's purpose includes promoting and enhancing a thriving credit union community.

70. Plaintiff Michigan Credit Union League ("Michigan CUL") is an association of credit unions headquartered in Michigan. Michigan CUL's purpose includes advocating on behalf of its members, fostering communications between credit unions, and providing high-quality solutions to help its members succeed.

71. Plaintiff Mississippi Credit Union League ("Mississippi CUL") is an association of credit unions headquartered in Mississippi. Mississippi CUL has 81 credit union members, which have approximately $5 billion in assets and are owned by over 600,000 consumers. Mississippi CUL's purpose includes advocating for its members, increasing their knowledge, and fostering their financial success.

72. Plaintiff Mountain West Credit Union Association ("Mountain West CUA") is a regional association of credit unions headquartered in Arizona. Mountain West CUA has 125 member credit unions, which have $34 billion in assets and are owned by 3.1 million consumers. Mountain West CUA's purpose

includes serving and supporting its membership through communications, community outreach, education, training, operational assistance, and advocacy.

73. Plaintiff New York Credit Union Association ("NYCUA") is an association of credit unions headquartered in New York. Its members are owned by more than 5 million consumers. NYCUA's purpose includes advocating for its members and advancing the credit union movement by advocating, educating and unifying the interests of its members statewide.

74. Plaintiff Credit Union Association of the Dakotas ("CUA of the Dakotas") is a regional association of credit unions headquartered in North Dakota. CUA of the Dakotas's purpose includes advocating for its members and helping them succeed.

75. Plaintiff Ohio Credit Union League ("Ohio CUL") is an association of credit unions headquartered in Ohio. Ohio CUL's credit union members have over $8 billion in assets and are owned by approximately 2.76 million consumers. Ohio CUL's purpose includes advocating for its members and providing them with compliance and information services, opportunities for educational and professional development, communications, media relations, and outreach.

76. Plaintiff Cornerstone Credit Union League ("Cornerstone") is a regional association of credit unions headquartered in Texas with more than 550

members. Cornerstone's purpose includes advocating for its members and advancing their success by promoting the growth, strength, and unity of credit unions.

77. Plaintiff Utah Credit Union Association ("Utah CUA") is an association of credit unions headquartered in Utah. Utah CUA's purpose includes advocating on behalf of its members and providing education, training, and community involvement services to help them prosper.

78. Plaintiff Virginia Credit Union League ("Virginia CUL") is an association of credit unions headquartered in Virginia. Virginia CUL has 160 member credit unions. Virginia CUL's purpose includes advocating for its members, preserving and promoting credit unions, and assisting its members to be preeminent providers of consumer financial services.

79. Plaintiff Wisconsin Credit Union League ("Wisconsin CUL") is an association of credit unions headquartered in Wisconsin. Wisconsin CUL has 70 member credit unions, which have assets of approximately $28 billion and are owned by more than 2.4 million consumers. Wisconsin CUL's purpose includes serving Wisconsin's credit unions and promoting the credit union difference through advocacy, education, and public service.

80. The Association Plaintiffs are duly authorized to bring this action

against Home Depot. Many of the Association Plaintiffs' members do not have the time or resources to pursue this litigation and fear retribution if they become named plaintiffs. Home Depot has caused the Association Plaintiffs to expend their own resources assisting members injured by Home Depot's data breach, and they have otherwise been directly and adversely impacted.

Defendants

81. Defendant Home Depot U.S.A., Inc. is a Delaware corporation with its principal place of business in Atlanta, Georgia which operates as a subsidiary of The Home Depot, Inc.

82. Defendant The Home Depot, Inc. is a Delaware corporation with its principal place of business in Atlanta, Georgia. The Home Depot, Inc. is the parent of Defendant Home Depot, U.S.A., Inc.

83. As it relates to matters relevant to this litigation, The Home Depot, Inc. and Home Depot U.S.A., Inc. constitute a single entity. The parent and subsidiary share the same key executives and abide by the same corporate policies and procedures such that there is no semblance of independence between them. The Home Depot, Inc. exercises such control over the actions of Home Depot, U.S.A., Inc. that the subsidiary operates as nothing more than a division or department of the parent. To the extent that Home Depot U.S.A., Inc. is truly a

distinct entity, it acts as an agent of, or as a joint venturer with, its parent.

FACTUAL BACKGROUND

84. Home Depot describes itself as the world's largest home improvement retailer and sells a wide assortment of building and home improvement materials, tools, hardware, and other products. As of 2014, Home Depot operated more than 2,200 stores in North America. In its last fiscal year, Home Depot generated more than $83 billion in net sales and more than $6.3 billion in net earnings.

85. A large portion of Home Depot's sales are made to customers who use credit or debit cards.

86. When a customer uses a credit or debit card, the transaction involves four primary parties: (1) the "merchant" (such as Home Depot) where the purchase is made; (2) an "acquiring bank" (which typically is a financial institution that contracts with the merchant to process its payment card transactions); (3) a "card network" or "payment processor" (such as Visa and MasterCard); and (4) the "issuer" (which is a financial institution such as the Financial Institution Plaintiffs that issues credit and debit cards to its customers).

87. Processing a payment card transaction involves four major steps:

- *Authorization*: When a customer presents a card to make a purchase, Home Depot requests authorization of the transaction from the card's issuer.

- *Clearance*: If the issuer authorizes the transaction, Home Depot completes the sale to the customer and forwards a purchase receipt to the acquiring bank with which it has contracted.

- *Settlement*: The acquiring bank pays Home Depot for the purchase and forwards the receipt to the issuer, which then reimburses the acquiring bank.

- *Post-Settlement*: The issuer posts the charge to the customer's credit or debit account.

88. In processing payment card transactions, merchants acquire a substantial amount of information about each customer, including his or her full name; credit or debit card account number; card security code (the value printed on the card or contained in the microprocessor chip or magnetic stripe of a card and used to validate card information during the authorization process); the card's expiration date and verification value; and the PIN number for debit cards. This information typically is stored on the merchants' computer systems and transmitted to third parties to complete the transaction. At other times and for other reasons, merchants also may collect other personally identifiable information about their customers, including but not limited to financial data, mailing addresses, phone numbers, driver's license numbers, and email addresses. All of this information is collectively referred to as "personally identifiable information" or "PII."

89. For years, Home Depot has stored in its computer systems massive amounts of PII about its customers. Home Depot uses this information to process payment card transactions in connection with sales to its customers and to generate profits by such means as sharing the information with third-party affiliates, recommending additional services to customers, and employing predictive marketing techniques. As an asset having considerable value, PII about its customers is stored by Home Depot indefinitely.

90. Home Depot is – and at all relevant times has been – aware that the information it maintains about its customers is highly sensitive and could be used for nefarious purposes by third parties, such as perpetuating identity theft and making fraudulent purchases.

91. Home Depot also is – and at all relevant times has been – aware of the importance of safeguarding its customers' information and of the foreseeable consequences that would occur if its security systems were breached, specifically including the significant costs that would be imposed on its customers, issuers such as the Financial Institution Plaintiffs, and others.

92. Indeed, in 2008, Home Depot identified the potential repercussions of a data security breach as a substantial "Risk Factor" for its business in its annual report and SEC filings, stating:

> ***The regulatory environment related to information security and privacy is increasingly rigorous, and a significant privacy breach could adversely affect our business.***
>
> The protection of our customer, employee and company data is important to us. The regulatory environment related to information security and privacy is increasingly rigorous, with new and constantly changing requirements applicable to our business. In addition, our customers have a high expectation that we will adequately protect their personal information. A significant breach of customer, employee or company data could damage our reputation and result in lost sales, fines and lawsuits.

Home Depot made similar statements in its annual report and SEC filings each year since 2008.

93. In addition to its general duty to safeguard customers' information to prevent the risk of foreseeable harm to others, Home Depot is – and at all relevant times has been – obligated to safeguard such information by, among other things, rules governing payment card transactions, industry standards, various federal and state laws, and its own commitments, internal policies and procedures.

94. Home Depot has continuously acknowledged this legal duty and reassured the public its duty was being met in the company's "Privacy Policy" posted on its website. For example, the version of the policy in effect in April, 2014 told the public that Home Depot used "industry standard means" to protect customer information and that its security measures were "appropriate for the type of information we collect."

Home Depot's Long History of Inadequate Data Security

95. Home Depot's treatment of the sensitive personal and financial information entrusted to it has been woefully inadequate for years.

96. Up through and including the period during which the 2014 breach occurred, Home Depot's data security systems suffered from many deficiencies that made them vulnerable to hackers, including without limitation the following:

a. Home Depot failed to maintain an adequate firewall, which is necessary to prevent hackers from penetrating its systems;

b. Home Depot failed to have adequate internal controls to prevent unauthorized users from navigating freely and without detection around its computer network;

c. Home Depot failed to restrict access to cardholder data on its network to those with a business need-to-know;

d. Home Depot failed to use coded numbers to disguise the point-of-sale terminals in its stores' self-checkout lanes, which make it more difficult for hackers to locate the terminals;

e. Home Depot failed to maintain and use up-to-date anti-virus software on its point-of-sale terminals, which prevents the installation of malware used by hackers to steal customer data;

f. Home Depot failed to encrypt cardholder data at the point-of-sale, which renders the data virtually useless to hackers;

g. Home Depot failed to adequately track access to its network and monitor the network for unusual activity, particularly at its point-of-sale terminals, which is necessary to detect the presence of hackers and take timely remedial action; and,

h. Home Depot failed to adequately scan the computer systems inside its stores for vulnerabilities that could be exploited by hackers.

Not surprisingly, the hackers responsible for the 2014 data breach took advantage of these very deficiencies.

97. Much of the blame for the state of Home Depot's data security systems can be placed squarely on the shoulders of the company's IT management, whose ineffective leadership was characterized by neglect, incompetence, and a desire to cut corners to save money, as well as on Home Depot's senior management who hired its IT managers and tolerated their poor performance.

98. Matthew Carey was responsible for Home Depot's information technology systems during the relevant time. He was hired as Home Depot's Chief Information Officer ("CIO") in 2008 and reported to Home Depot's CEO. Carey's primary background and focus was in the area of IT infrastructure and software

development, not data security. At Home Depot, Carey's principal interest in data security was using it as an area for cost-cutting.

99. Carey's principal deputy – the person with direct responsibility for data security during much of the relevant time period – was Jeff Mitchell. He joined Home Depot in 2009, one year after he had been fired as the director of IT security and architecture at Lowe's Home Improvement. In August, 2011, Mitchell was promoted to Senior Director of IT Security and thereafter served in the role of Chief Information Security Officer. Within three months of Mitchell's promotion, approximately half of Home Depot's IT security employees quit, largely out of frustration with his poor management.

100. Ricky Joe Mitchell was also given substantial responsibility for data security at Home Depot. (Ricky Joe Mitchell is no relation to Jeff Mitchell. For clarity, this complaint will refer to Jeff Mitchell as "Mitchell" and identify Ricky Joe Mitchell by his full name.) Ricky Joe Mitchell started at Home Depot in 2012 and about one year later was promoted to Senior Architect for IT Security, a position from which he oversaw data security systems at the company's stores. One month before he was hired by Home Depot, Ricky Joe Mitchell had been fired by his previous employer. Two months after being promoted by Home Depot, he was indicted on federal charges for intentionally sabotaging his former employer's

computers, causing the company to cease operations for a month and lose in excess of $1 million. In January, 2014, Ricky Joe Mitchell pled guilty and was sentenced to four years in prison.

101. Carey, Mitchell, Ricky Joe Mitchell and other managers were aware of Home Depot's data security problems. However, they routinely failed to heed warnings about the problems, shelved remedial projects undertaken by IT staff, and discouraged IT staff from recommending improvements. Further, their inaction, emphasis on cutting costs at the expense of basic security needs, and overall management style created turmoil. As a result, competent employees were driven away, making Home Depot's data security problems worse.

Home Depot Often Ignored Warnings
About Data Security Problems

102. Home Depot was repeatedly warned about the deficiencies and vulnerabilities in its systems before the data breach occurred in 2014.

103. Home Depot's IT employees began reporting data security problems beginning in 2008, if not earlier, telling supervisors that Home Depot's computer systems were "easy prey for hackers" and could be breached by anyone with "basic internet skills."

104. Beginning in 2009, nearly five years before the breach, computer experts repeatedly warned Home Depot about the failure to encrypt customer data

at the point-of-sale. Because of the lack of encryption, after a customer's payment card was swiped, the data on the card's magnetic stripe was visible in clear text (and thus vulnerable to hackers) while being sent to Home Depot's main servers. Point-of-sale encryption scrambles the data into a format called "cipher text" so that, even if stolen immediately after the card is swiped, the data cannot be read by hackers. Although Home Depot had the capability to implement point-of-sale encryption, its management refused to authorize its implementation, citing the cost and operational disruption.

105. In 2010, an employee discovered a major security flaw involving devices used by Home Depot's in-store sales force. This flaw allowed unauthorized persons to gain access to Home Depot's network and, once inside, navigate freely without triggering any alarms. The employee repeatedly warned Home Depot in writing about the risk to confidential customer financial information and the need to take immediate remedial action. After largely ignoring the employee for months, Home Depot put a stop to the warnings by firing the employee. Home Depot did not fix the problem.

106. Furthermore, despite pleas from security staffers, Home Depot failed to properly implement and update antivirus software for its point-of-sale systems. At the time of the data breach in 2014, Home Depot was using "Symantec

Endpoint Protection 11," antivirus software that had been issued in 2007. Symantec released a new version of the software in 2011 because, according to Symantec, the "threat landscape had changed significantly" and the new product would better protect against the "explosion in malware scope and complexity." Nonetheless, Home Depot failed to purchase the new version. Inexplicably, Home Depot also failed to turn on a feature of the 2007 version of the Symantec antivirus software designed specifically to spot the kind of malware that attacks point-of-sale terminals. Because of concern about Home Depot's approach to data security, three of Symantec's contractors refused to continue working for Home Depot, and Symantec threatened to cease doing business with the company.

107. Another major area of concern involved Home Depot's failure to adequately monitor its network for potential vulnerabilities, abnormalities, and the presence of malware. Employees repeatedly warned Carey and Mitchell that Home Depot's efforts were inadequate and recommended that remedial steps be taken. For example, employees complained about the lack of bandwidth on the network, which prevented the security logs for point-of-sale terminals from being uploaded so that they could be reviewed at corporate headquarters rather than in the stores. Employees also complained that only ten percent of Home Depot's store computers were being scanned for vulnerabilities. Yet, Carey and Mitchell

consistently refused to take action or authorize recommended improvements.

108. Management also routinely ignored other suggestions about upgrading Home Depot's data security systems to better protect the confidential information of its customers and failed to prioritize the installation of patches to fix software bugs and security vulnerabilities.

Management Actively Interfered with Efforts to Improve Data Security

109. In addition to ignoring warnings about deficiencies in its data security systems, Home Depot's IT management took affirmative steps to prevent IT staff from fixing the deficiencies and made it known that Home Depot did not intend to spend the money to make necessary improvements.

110. For example, shortly after being promoted, Mitchell terminated a project begun by his predecessor in early 2011 to fully encrypt customer data throughout the payment card cycle, including at the point-of-sale. This project was essential to eliminate a major deficiency about which Home Depot had been warned for several years. As a result of the project's termination, customer data remained unencrypted and vulnerable to attack.

111. Another project shelved by Mitchell involved implementation of the "Symantec Control Compliance Suite," software that was needed to improve the ability to monitor the security of Home Depot's network. The software would

have automated the monitoring process, allowing the network to be assessed centrally, using consistent standards, and much more frequently. Instead, because the software was not implemented, IT staff had to continue using a tedious, manual process that left the network far more vulnerable. When IT staff asked when the project would be revived, Mitchell told them, "We will get to it when we get to it" or "Matt [Carey] said to leave it alone."

112. Mitchell also shelved a project that would have better protected "privileged accounts" on the network – i.e. those accounts with enhanced credentials that allow broader access to servers, databases and infrastructure. Home Depot had a four year relationship with Israel-based CyberArk Software Ltd., which designed software to better protect privileged accounts from being infiltrated, and had decided to install the software to improve the security of its network. The project was abandoned despite the fact that employees had worked on it for months and the software licensing fees had already been paid.

113. Before Mitchell's promotion, Home Depot required a detailed assessment of every new IT product under consideration that was documented in a Memorandum of Records and Requirements ("MORR"). The MORR assessment identified and analyzed potential security risks related to the product. If the potential security risks were high, then Home Depot required upper-level

management to approve the decision whether or not to purchase the product. After Mitchell began serving in the role of Chief Information Security Officer, Home Depot stopped performing MORR assessments, thus eliminating another means of identifying vulnerabilities in Home Depot's data security systems.

114. Home Depot also maintained what was known as the "Security Review Board," a group of IT experts that was charged with, among other things, deciding whether to implement employee recommendations for improvements to data security systems. While neither Mitchell nor Carey were members, the Security Review Board could only act at their direction, and Carey was required to personally approve the board's decisions. After Mitchell's promotion, he and Carey used their power to thwart efforts by the Security Review Board to improve data security. One of the recommendations they killed was to implement point-of-sale encryption at all Home Depot stores.

115. Mitchell actively discouraged employees from raising questions about or suggesting improvements to Home Depot's data security systems. After Security Review Board meetings, he routinely confronted employees who expressed concerns or proposed new security measures, asking them: "Why are you trying to change the environment?" In response to continuing recommendations to encrypt customer data at the point-of-sale terminals, Mitchell

repeatedly told staff, "it's going to interrupt the business" or "it's more of an expense" than it is worth.

116. Mitchell also told staff they needed to settle for "C-level security" (as opposed to A-level or B-level security) because security updates would be costly and might disrupt operations. Such comments were intended to create a culture of complacency at Home Depot and dissuade IT employees from recommending fixes to the data security problems. Mitchell's efforts largely succeeded. Former IT employees reported that, at Home Depot, data security was an "afterthought" and "just a check-mark" on management's to-do list.

117. Given Home Depot's lack of concern with data security and its treatment of those who advocated for improvements, it is no surprise that one former IT security employee went so far as to warn friends to use cash, rather than credit cards, at Home Depot's stores in the months before the 2014 data breach.

Home Depot's Approach to Data Security
Caused Turmoil Within the Company

118. Management's repeated failure to make needed improvements to Home Depot's data security systems, efforts to undercut ongoing projects, and Mitchell's bullying, abrasive and polarizing management style caused turmoil within the company which further contributed to its data security problems.

119. From August, 2011, when Mitchell was promoted through November, 2011, approximately thirty of the sixty employees working on data security issues left Home Depot. The departures included employees tasked with finding security flaws in the network and ensuring Home Depot met industry security standards.

120. Even before Mitchell's promotion, Home Depot's data security operations were understaffed. Home Depot rarely employed more than fifty or sixty IT security personnel at any given time. In contrast, other companies of comparable size typically employ hundreds or thousands of such personnel. As a result of the mass departures in 2011, the burden on the remaining employees increased significantly, making it even harder to protect the network and more likely problems would go undetected.

121. In early 2012, the remaining data security employees were so fed up with Mitchell's leadership and Home Depot's continuing problems with data security that they tried to go over his head. The employees met as a group with Mitchell's immediate supervisor, Matthew Carey, in a conference room near Carey's office. The staffers presented Carey with a report detailing Home Depot's security deficiencies, including the lack of encryption at point-of-sale terminals. Carey dismissed the staff's concerns, explained that cost-cutting was a necessity, and made no changes. Thereafter, even more IT staffers quit.

122. The pattern of high turnover continued into 2013. In the spring of that year, four of the eight people responsible for ensuring that credit card data was encrypted as it traveled over Home Depot's network left the company. The four left, in part, because they were frustrated that management would not address their concerns about the vulnerability of the network.

123. By the time of the data breach in 2014, ineffective and unresponsive management and mounting frustration with Home Depot's lack of concern for data security had effectively driven off many, if not most, of the competent IT staff who had experience dealing with the company's data and systems. Moreover, Symantec, one of Home Depot's top security vendors, had told Mitchell that even it would stop working for Home Depot unless the company took security more seriously.

124. Home Depot's approach to data security issues and the resulting frustration of IT staff and third-party security vendors was perhaps best epitomized by a phrase often heard from Carey in denying requests for training, new software, and other improvements: "We sell hammers."

Leading Up to the 2014 Data Breach, Home Depot Ignored Increasing Red Flags Signaling that its Network was Vulnerable to Hackers

125. In the nine months leading up to the 2014 data breach, a series of red flags should have put Home Depot on high alert about the risk of an impending

company-wide data breach. Instead, consistent with its corporate culture, Home Depot reacted complacently, if at all, and, when the company finally realized it had a major problem, failed to move quickly enough to implement a fix.

126. Home Depot suffered a small data breach in July 2013 when data-stealing malware was placed on at least eight point-of-sale terminals at a Home Depot store in Texas. This incident emphasized that the terminals had security weaknesses and should have alerted Home Depot to the possibility that hackers were testing its systems.

127. In August of 2013, Visa sent a letter to Home Depot entitled "Retail Merchants Targeted by Memory-Parsing Malware." The letter warned:

> Since January 2013, Visa has seen an increase in network intrusions involving retail merchants. Once inside the merchant's network, the hacker will install memory parser malware on the Windows based cash register system in each lane.

Yet, Home Depot took no action to upgrade its antivirus software, encrypt data at the point-of-sale, or make other security improvements.

128. On October 1, 2013, IT security consultant FishNet Security warned Home Depot that its computer systems were vulnerable because the Symantec Network Threat Protection ("NTP") firewall had been shut off in favor of a firewall packaged with Microsoft Windows. FishNet's report, among other things, stated that "It is highly advised and recommended the NTP Firewall component be

deployed and that Windows Firewall be discontinued" and that in order for the firewall to work properly "NTP was needed on all Home Depot computers, including register payment terminals." Notwithstanding that this report mirrored Visa's earlier warning about problems with the Windows firewall, Home Depot took no immediate action.

129. In December, 2013, Home Depot discovered that point-of-sale terminals at one of its stores in Columbia, Maryland were infected with malware known as "Infostealer," which siphons payment card data and forwards it to a remote location. Infostealer is exactly the type of malware that the Symantec NTP firewall is designed to block. The incident was another signal that hackers might be planning an attack on Home Depot and again emphasized the need to switch from the Windows to the Symantec NTP firewall. Yet, Home Depot still did not make the switch.

130. In December, 2013, Home Depot also received an urgent wake-up call when a massive data breach occurred at the nation's second largest retailer, Target Corporation. Hackers used the credentials of a third-party vendor to install malware on Target's in-store cash registers and steal payment card information of 40 million customers and other personal information of an additional 70 million people. The Target data breach received worldwide attention and put the entire

retail industry on notice that lax IT security could be exploited on a massive scale.

131. Following the Target data breach, Home Depot executives, led by then CEO Frank Blake, assembled a task force to devise a plan to avoid a similar fate. Blake requested Carey and IT personnel working under his direction to prepare a report explaining what Home Depot needed to do to prevent hackers from infiltrating its systems. The task force was also charged with putting together a "playbook" on how to respond to a data breach if one occurred.

132. While the task force was at work, Home Depot received still more red flags warning of the deficiencies of its data security system and the potential for a massive data breach.

133. In January, 2014, an outside security consultant – Solutionary – reported to Mitchell that Home Depot's network was vulnerable to attack and did not comply with industry standards.

134. Also in January, 2014, the Federal Bureau of Investigation distributed a confidential report to Home Depot entitled "Recent Cyber Intrusion Events Directed Toward Retail Firms." The report pointedly warned of the risk posed by malware installed on point-of-sale systems to steal cardholder data and stated:

> We believe POS malware crime will continue to grow over the near term, despite law enforcement and security firms' actions to mitigate it . . . The accessibility of the malware on underground forums, the affordability of the software and the huge potential profits to be made

> from retail POS systems in the United States make this type of financially motivated cybercrime attractive to a wide range of actors.

The FBI's report re-emphasized the urgency of taking steps to improve security, such as upgrading the Symantec antivirus software, activating all of the software's features, replacing the Windows firewall, and encrypting data on point-of-sale terminals.

135. In February, 2014, FishNet issued another report to Home Depot urging it to deploy Symantec NTP on its point-of-sale devices in order to strengthen its defenses against a data breach.

136. That same month, the task force formed after the Target data breach made its recommendations about how to improve Home Depot's data security systems., which included:

a. Implementing stronger security-threat detection software;

b. Upgrading Home Depot's security operations center;

c. Purchasing intelligence feeds on hacker behavior;

d. Installing regularly-updated security "patches";

e. Upgrading software on Home Depot's point-of-sale terminals;

f. Implementing technology to encrypt payment card data on point-of-sale terminals.

Most of these recommendations had been previously rejected by Carey and other executives. Indeed, the task force's recommendations mirrored much of what Home Depot's employees, outside consultants, vendors and others had been recommending for years.

137. Despite the obvious risk of delay and specific warnings in the months before the breach, Home Depot failed to immediately upgrade its antivirus software, activate all of its security features, or replace the Windows firewall with Symantec's NTP product. As a result, at the time the hackers attacked, Home Depot was still running outdated antivirus software and using a flawed firewall. While Blake eventually gave the green light to implement point-of-sale encryption technology, the project did not get underway until after the hackers were already deep in Home Depot's systems.

The Home Depot Data Breach: April to September, 2014

138. Beginning in approximately April, 2014, hackers gained access to Home Depot's computer systems by using the credentials of a third-party vendor. The hackers then jumped the barrier between the "peripheral third-party system" and Home Depot's main computer network. The jump was possible because of the flaw with the Windows firewall about which Home Depot had been warned.

139. Once inside Home Depot's main computer network, the hackers were

able to "elevate" their credentials, act as if they were employees with privileged accounts, and navigate freely around the network without triggering any alarms. The hackers found Home Depot's point-of-sale systems and targeted 7,500 of its self-checkout lanes because the terminals were readily identifiable on the network. The cash registers staffed by Home Depot employees, in contrast, were identified only by numbers and thus more difficult for the hackers to find.

140. After locating the self-checkout registers, the hackers installed malware that operated similarly to the malware used in the Target data breach. Specifically, the malware siphoned off the information from a payment card when it was swiped on a Home Depot self-checkout terminal. The information was then collected by the hackers.

141. The malware remained on Home Depot's self-checkout terminals – and thus hackers were able to continue stealing the card data of customers who used the terminals – until approximately September 7, 2014, a period of roughly five months. The data breach went wholly undetected by Home Depot.

142. In late April, 2014, unaware that hackers had already exploited the gaping holes in Home Depot's security systems, the data breach task force was putting the finishing touches on a 45-page "playbook" about how to respond to a

data breach if one did occur. After the breach had been discovered, then CEO Blake admitted, "The irony was not lost on us."

143. In July, 2014, while the data breach was in full swing but as yet still undetected, Home Depot contracted with Symantec to perform a "health check" on its computer systems. The health check identified as critical issues that Home Depot was using out-of-date antivirus software and malware detection systems on its point-of-sale terminals. Home Depot should have responded immediately by upgrading this software, as it had been urged to do many times before. But Home Depot failed to upgrade its software, and the breach continued uninterrupted.

144. By the end of August, 2014, and still unbeknownst to Home Depot, hackers had been stealing the payment card information of its customers at the point-of-sale for roughly five months. During that time, the hackers acquired cardholder data belonging to tens of millions of Home Depot's customers.

145. On September 1, 2014, the website Rescator.cc (now Rescator.cm), which has been dubbed the "Amazon.com of the black market," alerted customers that massive quantities of stolen debit and credit cards would go on sale the next day. Rescator, the same underground cybercrime shop that sold millions of stolen card numbers from the 2013 Target data breach, advised its customers: "Load your accounts and prepare for an avalanche of cash!"

146. On September 2, 2014, Rescator offered the stolen card data for sale in two batches under the name "American Sanctions." Later that day, security blogger Brian Krebs of "Krebs on Security" broke the news that banks were seeing evidence of fraud on customer accounts with the common link being purchases at Home Depot.

147. The two batches of cardholder data on Rescator reportedly sold for between $50 to $100 per card and claimed a 100 percent validity rate, meaning that the card numbers were valid and working. Specialty cards such as "platinum" and "business" credit cards commanded higher prices, while debit cards generally sold for less. The Rescator website, valued by cybercriminals for its customer service and ease of use, even temporarily crashed because it received so many hits.

148. On September 2, 2014, the U.S. Secret Service alerted Home Depot executives that its computer systems likely had been breached. In response, Home Depot issued a statement buried on its website noting that it was "looking into some unusual activity" and that it would provide "further information as soon as possible." Home Depot did not confirm that a breach had occurred.

149. On September 3, 2014, Krebs, *not* Home Depot, reported that nearly all Home Depot stores in the country were affected. By comparing the ZIP code data available for the stolen cards on the Rescator website to the ZIP code

locations of Home Depot's stores, Krebs was able to establish "a staggering 99.4 percent overlap" -- all but confirming that Home Depot was the source of the data breach. Despite this overwhelming evidence, Home Depot still did not publicly disclose its systems had been breached.

150. On September 4, 2014, three additional batches of stolen card numbers were made available on Rescator's website. Krebs also reported a sharp uptick in debit card fraud reported by banks and that the fraud, which in one case was upwards of $300,000 in just two hours, could be traced to cards that had all been recently used at Home Depot. Because Home Depot had not yet confirmed the breach, however, financial institutions were reluctant to cancel and reissue their payment cards, which resulted in the new batches still having a 100 percent validity rate.

151. On September 6, 2014, Home Depot's investigators discovered evidence that point-of-sale malware had been deleted from a Home Depot store computer and confirmed that a security breach had in fact taken place. Despite now having confirmatory evidence, Home Depot still did not publicly disclose that its systems had been breached.

152. On September 7, 2014, seven additional batches of stolen card numbers were made available on Rescator's website, resulting in a dramatic uptick

in debit and credit fraud for Home Depot customers. The new batches had a validity rate of nearly 100 percent because Home Depot had not yet confirmed the breach and, as a result, the overwhelming bulk of compromised payment cards had not yet been canceled.

153. Also on September 7, 2014, Krebs reported that the malware used by the Home Depot hackers was a variant of "BlackPOS," the malware used in the Target breach. Krebs noted: "Clues buried within this newer version of BlackPOS support the theory put forth by multiple banks that the Home Depot breach may involve compromised store transactions going back at least several months."

154. On September 8, 2014, six days after the data breach was first made public, Home Depot finally broke its silence and issued a news release on its website reporting that its computer systems had been breached. The news release confirmed that the breach was widespread, potentially impacting any person who had used a payment card at Home Depot stores in the United States or Canada since April of 2014, but failed to convey the severity of the breach and failed to warn that customers' financial information was currently for sale and being used by criminals around the world.

155. Home Depot's response to the breach was widely criticized by industry experts. One expert concluded: "Honestly, Home Depot is in trouble here

. . . This is not how you handle a significant security breach." The breach itself bore many similarities to the one that occurred at Target, a fact that was particularly damaging for Home Depot. Said one security expert: "Everyone should have learned from what happened to Target . . . And the fact they haven't should be quite damning."

156. After the breach was announced, Attorneys General for California, Connecticut, Illinois, Iowa, Massachusetts, New Hampshire, New York, and Rhode Island launched a probe into Home Depot's conduct.

157. The breach also drew criticism from federal officials. For example, two U.S. Senators -- Sen. Richard Blumenthal of Connecticut and Sen. Ed Markey of Massachusetts -- called for the Federal Trade Commission ("FTC") to investigate and questioned Home Depot's efforts to protect its customers' data. According to the Senators:

> Online discussions of vulnerabilities on Home Depot's website date back to 2008. These revelations raise serious concerns about Home Depot's responsiveness to potential attacks, particularly in light of other retailers that have recently been targeted by hackers…Given the unprecedented scope and extended duration of Home Depot's data breach, it appears that Home Depot may have failed to employ reasonable and appropriate security measures.

The senators went on to say: "If Home Depot failed to adequately protect customer information, it denied customers the protection that they rightly expect

when a business collects such information. Such conduct is potentially unfair and deceptive…"

Home Depot's Failure to Correct Security Problems, About Which it Knew, Caused the Data Breach

158. On November 6, 2014, Home Depot issued a news release announcing the results of what it described as a two-month internal investigation. The release explained how the breach allegedly occurred and acknowledged, for the first time, that approximately 53 million email addresses had also been stolen.

159. In the release, then CEO Blake admitted Home Depot was to blame for the breach, stating: "If we rewind the tape, our security systems could have been better. Data security just wasn't high enough in our mission statement." Blake also admitted the company's systems were "desperately out of date."

160. Blake is correct. The breach occurred because of Home Depot's longstanding approach to data security and its failure to fix major vulnerabilities in its security systems about which it knew and had been warned, such as:

a. The ability of outsiders to access Home Depot's network using the login credentials of a third-party vendor and then "elevate" the credentials to navigate the company's network freely and undetected;

b. The failure to identify terminals in the self-checkout lanes with

coded numbers, making them more difficult for hackers to find on the network;

c. The failure to upgrade the out-of-date Symantec antivirus software as had been recommended by the manufacturer;

d. The failure to activate an important feature of the Symantec antivirus software specifically designed to prevent the installation of the type of malware used in the breach;

e. Continued use of the discredited Windows firewall rather than activating Symantec's NTP firewall on its point-of-sale terminals;

f. The lack of effective monitoring of the network for potential vulnerabilities, malware, and unusual activity signaling that hackers were active (including the failure to run vulnerability scans on 90 percent of Home Depot's stores and enable security logs on the point-of-sale terminals so they could be reviewed centrally); and,

g. The failure to encrypt cardholder data on the point-of-sale terminals.

161. The data breach also was facilitated by Home Depot's decisions to cut corners and shelve ongoing projects such as the installation of encryption

technology at the point-of-sale, the CyberArk software that would have made it more difficult for the hackers to break into privileged accounts, and the Symantec Control Compliance Suite that would have automated security assessments.

162. Home Depot's incompetence while the breach was occurring also increased the amount of stolen cardholder data. For example, the malware installed by the hackers disguised itself as a McAfee antivirus program to avoid detection. Home Depot did not use McAfee antivirus software, so the presence of a McAfee-like program on its systems should have sounded alarm bells if Home Depot had been properly monitoring its network. However, because Home Depot did not properly monitor its network, the company failed to notice the malware, allowing the breach to continue and increasing the amount of card data that was stolen.

163. Furthermore, the failures of Home Depot's officers and directors contributed to the data breach. The damage resulting from the data breach likely would have been avoided or reduced if Home Depot's officers and directors had met their fiduciary duties to the company and its shareholders, properly overseen the activities of their subordinates, not allowed the corporate culture of neglect and incompetence to continue for years, and followed recommendations of the National Institute of Standards and Technology relating to the critical role of cybersecurity

in corporate governance.

164. That Home Depot had the ability to fix its data security problems and could easily have done so before the breach occurred but for a lack of effective leadership at the highest levels of the company is illustrated by the delay in installing point-of-sale encryption technology. As described above, Carey had been warned for years of the critical importance of point-of-sale encryption; and in February, 2014 the task force specifically recommended that the technology be implemented to prevent a data breach such as the one that had occurred at Target. Yet, as of early September, 2014, roughly seven months later, the technology only had been installed at 25 percent of Home Depot's stores.

165. The failure to install the encryption technology promptly was not due to any technological hurdles, but simply due to Home Depot's neglect and incompetence. Upon learning its network had been breached, Home Depot was able to install the technology at the remaining 75 percent of its stores and have the technology tested and validated by two independent IT security firms *in eleven days*. If Home Depot had acted with such urgency earlier, the breach likely would have been avoided entirely.

Home Depot Violated Its Own Policies,
Industry Standards, and Other Security Requirements

166. In failing to prevent the data breach and minimize its impact, Home

Depot violated its own policies and commitments, industry standards, and regulatory requirements in the years before, and at the time of, the data breach.

Home Depot Failed to Follow its Own Policies and Procedures

167. At the time of the breach, Home Depot's internal policies and procedures required that customer information be kept confidential, that system vulnerabilities be mitigated in a timely manner, that necessary software upgrades be implemented, and that data be encrypted. Home Depot violated these policies and procedures in the years leading up to the 2014 data breach and during the commission of the breach itself by failing to maintain the confidentiality of its customer information, mitigate system vulnerabilities in a timely manner, upgrade security software, and encrypt customer data at the point-of-sale.

168. Home Depot also violated the terms of its Privacy Policy, specifically its assurances that the company was using "industry standard means" to protect customer data and that security measures were "appropriate for the type of information" being collected. In fact, Home Depot did not use industry standard means of protecting customer data, but rather ignored basic requirements of applicable industry standards. Home Depot also did not use appropriate security measures, but rather routinely failed to adopt appropriate security measures that were recommended by its own employees and consultants.

Home Depot Failed to Follow Card Operating Regulations

169. Payment card processors and networks, including Visa and MasterCard, issue Card Operating Regulations that are binding on Home Depot. Such regulations were in place long before the 2014 data breach.

170. The Card Operating Regulations required Home Depot to protect cardholder data and prevent its unauthorized disclosure; prohibited Home Depot from storing such data, even in encrypted form, longer than necessary to process the transaction; and mandated compliance with industry standards.

171. Home Depot violated the Card Operating Regulations because it failed to maintain the security and confidentiality of its customers' payment card information, inappropriately stored cardholder data, and as explained in more detail below violated industry standards.

Home Depot Violated Industry Standards

172. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS is *the* industry standard governing the security of payment card data, although it sets the minimum level of what must be done, not the maximum.

173. PCI DSS 3.0, the version of the standards in effect at the time of the 2014 data breach, imposed the following twelve "high-level" mandates:

PCI Data Security Standard – High Level Overview

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 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

PCI DSS 3.0, furthermore, set forth detailed and comprehensive requirements that had to be followed to meet each of the twelve mandates.

174. Among other things, PCI DSS required Home Depot to properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data to those with a need to know; establish a process to identify and timely fix security vulnerabilities; assign unique identification numbers to each individual with access to its systems; and encrypt payment card data at the point-of-sale.

175. At the time of the 2014 data breach, Home Depot was in violation of

PCI DSS 3.0, including each of the requirements set forth in the preceding paragraph. Indeed, in its 2015 Form 10-K filed with the SEC, Home Depot acknowledged that "the forensic investigator working on behalf of the payment card networks alleged that we were not in compliance with certain of [the PCI DSS] standards at the time of the 2014 data breach."

176. That Home Depot failed to comply with PCI DSS at the time of the breach is not surprising given its lackadaisical, unreasonable, and inadequate approach to data security. In fact, before the breach, Home Depot had a history of violating PCI DSS, failing to correct violations brought to its attention, and otherwise disregarding the importance of complying with industry standards.

177. For example, in 2011 Home Depot hired a Qualified Security Assessor ("QSA") – a company approved by the PCI Council to assess compliance with PCI DSS – to audit its data security systems. The QSA identified a "major gap" in Home Depot's data security, raising serious concerns about the safety of its customers' financial data, and recommended that the deficiencies be immediately addressed. While Home Depot represented it would comply with the recommendations in order to ease the concerns of the PCI Council, it failed to fully fix the deficiencies.

178. In 2012, Solutionary worked for Home Depot as its QSA. Home

Depot employees submitted a detailed PowerPoint presentation to Mitchell reporting that Home Depot had misrepresented to Solutionary the extent of Home Depot's security procedures and that Home Depot was not PCI DSS compliant. Upon receiving the report, Mitchell dismissed the findings and denied any wrongdoing by Home Depot.

Home Depot Failed to Comply with FTC Requirements

179. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

180. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of

data being transmitted from the system; and have a response plan ready in the event of a breach.

181. The FTC also has published a document entitled "FTC Facts for Business" which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

182. And the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

183. In the years leading up to the 2014 data breach and during the course of the breach itself, Home Depot failed to follow the guidelines recommended by the FTC. Further, by failing to have reasonable data security measures in place, Home Depot engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

Home Depot Failed to Comply with Other Legal Requirements

184. Several states have enacted data breach statutes that require merchants to use reasonable care to guard against unauthorized access to customer information, such as California Civil Code § 1798.81.5(b) and Wash. Rev. Code. § 19.255, or that otherwise impose data security obligations on merchants, such as

Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64. States have also adopted unfair and deceptive trade practices acts which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. And most states, including Georgia, *see* O.C.G.A. 10-1-911 *et seq.*, have enacted statutes requiring merchants to provide notice if their data security systems are breached. These statutes, implicitly or explicitly, support the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

185. For the reasons set forth in detail above, Home Depot failed to have reasonable security protections in place at the time of the 2014 breach and failed to provide timely notice of the breach. As a result, Home Depot violated the terms of the statutes described in the preceding paragraph.

The Data Breach Damaged Financial Institutions

186. The data breach caused substantial damage to the Financial Institution Plaintiffs and class members, who had to act immediately to mitigate the massive fraudulent transactions being made on payment cards that they had issued, while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but the Financial Institution Plaintiffs and class members are not. Financial institutions bear primary responsibility for reimbursing

customers for fraudulent charges on the payment cards they issue.

187. As a result of the Home Depot data breach, the Financial Institution Plaintiffs and class members have been forced to cancel and reissue payment cards, change or close accounts, notify customers that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage. And debit and credit cards belonging to class members and the Financial Institution Plaintiffs – as well as the account numbers on the face of the cards – were devalued.

188. The financial damages suffered by the Financial Institution Plaintiffs and class members are massive and continue to increase.

189. In October 2014, CUNA estimated that 7.2 million cards issued by credit unions were compromised, that credit unions incurred $60 million in reissuance costs, and that the approximate replacement cost per card was $8.02. On December 18, 2014, the Independent Community Bankers of America estimated that community banks were forced to reissue nearly 7.5 million cards at a cost of more than $90 million. Because credit unions and community banks issued only a portion of the cards that were compromised by the breach, the total

reissuance costs incurred by all financial institutions is much higher.

190. Industry sources have also attempted to estimate the fraud losses resulting from the breach. Based on prior thefts of customer information, credit card firm BillGuard predicts that an average of $332 in fraudulent charges will be made on each card used by the thieves and that the total fraud losses will approximate $3 billion.

191. More precise calculations of the costs of reissuance, fraud losses, and other financial losses collectively suffered by the Financial Institution Plaintiffs and absent class members will be made during the course of this litigation.

CLASS ACTION ALLEGATIONS

192. The Financial Institution Plaintiffs bring this action pursuant to Rules 23(a) and 23(b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and a national class described as the Financial Institution National class (the "FI National Class"), which is defined as:

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present.

193. In addition to the FI National Class, the Financial Institution Plaintiffs seek to bring eight state subclasses that assert claims under statutes specific to each

state defined as follows:

> **Alaska Subclass:** All banks, credit unions, financial institutions, and other entities in the State of Alaska that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present (the "Alaska Subclass").
>
> **California Subclass:** All banks, credit unions, financial institutions, and other entities in the State of California that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present (the "California Subclass").
>
> **Connecticut Subclass:** All banks, credit unions, financial institutions, and other entities in the State of Connecticut that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present (the "Connecticut Subclass").
>
> **Florida Subclass:** All banks, credit unions, financial institutions, and other entities in the State of Florida that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present (the " Florida Subclass").
>
> **Illinois Subclass:** All banks, credit unions, financial institutions, and other entities in the State of Illinois that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present (the " Illinois Subclass").
>
> **Massachusetts Subclass:** All banks, credit unions, financial institutions, and other entities in the Commonwealth of Massachusetts that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present (the "Massachusetts Subclass").

> **Minnesota Subclass:** All banks, credit unions, financial institutions, and other entities in the State of Minnesota that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present (the "Minnesota Subclass").
>
> **Washington Subclass:** All banks, credit unions, financial institutions, and other entities in the State of Washington that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present (the "Washington Subclass").

194. Alternatively, in the event that the FI National Class is not certified, the Financial Institution Plaintiffs seek to certify forty-five separate, state specific classes in the District of Columbia and all states except Arizona, Kentucky, Nebraska, North Dakota, South Dakota, and Vermont. The class in each state is defined as follows:

> All banks, credit unions, financial institutions, and other entities in [insert the name of the specific state] that issued payment cards (including debit or credit cards) used by customers to make purchases from Home Depot during the period from April 1, 2014 to the present.

The alternative state law classes would bring on a state-by-state basis the same claims being asserted nationally by the FI National Class; that is, claims for negligence and negligence *per se*.

195. All of the classes described above, including the FI National Class, the eight state subclasses, and the alternative state specific classes are collectively referred to in this complaint as the "classes."

196. The definitions of the classes may be modified as new details emerge through discovery and based upon rulings of the Court.

Rule 23(a)

197. This action may properly be maintained on a class basis and satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

198. The members of the classes are so numerous that joinder of all members would be impracticable. Plaintiffs do not know the precise number of members in the various classes, but believe that there are more than 5,000 members in the FI National Class and at least fifty or more in each state class and subclass.

199. There are common questions of law and fact that predominate over questions affecting only individual class or subclass members. These common legal and factual questions, include, but are not limited to:

- Whether Home Depot owed a duty to Plaintiffs and members of the classes to protect cardholder personal and financial data;
- Whether Home Depot failed to provide adequate security to protect consumer cardholder personal and financial data;
- Whether Home Depot negligently or otherwise improperly

allowed cardholder personal and financial data to be accessed by third parties;

- Whether Home Depot failed to adequately notify Plaintiffs and members of the classes that its data system was breached;
- Whether Plaintiffs and members of the classes were injured and suffered damages and ascertainable losses;
- Whether Home Depot's failure to provide adequate security proximately caused Plaintiffs' and class members' injuries;
- Whether Plaintiffs and members of the classes are entitled to damages and, if so, the measure of such damages; and
- Whether Plaintiffs and members of the classes are entitled to declaratory and injunctive relief.

200. The claims of the Financial Institution Plaintiffs are typical of the claims of the absent class members and have a common origin and basis. The Financial Institution Plaintiffs and absent class members are all financial institutions injured by Home Depot's data breach. The Financial Institution Plaintiffs' claims arise from the same practices and course of conduct giving rise to the claims of the absent class members and are based on the same legal theories. If prosecuted individually, the claims of each class member would necessarily rely

upon the same material facts and legal theories and seek the same relief.

201. The Financial Institution Plaintiffs will fully and adequately assert and protect the interests of the absent class members and have retained class counsel who are experienced and qualified in prosecuting class action cases similar to this one. Neither the Financial Institution Plaintiffs nor their attorneys have any interests contrary to or conflicting with the interests of absent class members.

Rule 23(b)(3)

202. The questions of law and fact common to all class members predominate over any questions affecting only individual class members.

203. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent 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. Class treatment will also permit class members to litigate their claims where it would otherwise be too expensive or inefficient to do so. Plaintiffs know of no difficulties in managing this action that would preclude its maintenance as a class action.

204. Addresses and other contact information for each class member is readily available, facilitating notice of the pendency of this action.

COUNT I
Negligence
On Behalf of the FI National Class and the Alternative State Specific Classes

205. Home Depot owed – and continues to owe – a duty to the Financial Institution Plaintiffs, the FI National Class and the alternative state specific classes to use reasonable care in safeguarding PII and to notify them of any breach in a timely manner so that compromised financial accounts and credit cards can be closed quickly in order to avoid fraudulent transactions. This duty arises from several sources, including but not limited to the sources described below, and is independent of any duty Home Depot owed as a result of its contractual obligations.

206. Home Depot has a common law duty to prevent the foreseeable risk of harm to others, including the Financial Institution Plaintiffs, the FI National class, and alternative state specific classes. That injury would result from Home Depot's failure to use reasonable measures to protect PII and to provide timely notice of a breach was clearly foreseeable. Indeed, Home Depot has recognized the substantial risk of such injury in its annual reports since 2008. It also was foreseeable that, if reasonable security measures were not taken, hackers would

steal PII belonging to millions of Home Depot's customers; thieves would use the PII to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud, such as by cancelling and reissuing the compromised cards, and to reimburse their customers for fraud losses; and that the resulting financial losses would be immense.

207. Home Depot assumed the duty to use reasonable security measures as a result of its conduct, internal policies and procedures, and Privacy Policy in which the company stated it was using "industry standards means" of protecting PII and that its security measures were "appropriate for the type of information we collect." By means of these statements, Home Depot specifically assumed the duty to comply with industry standards, including PCI DSS.

208. A duty to use reasonable security measures arose as a result of the special relationship that existed between Home Depot and the Financial Institution Plaintiffs, the FI National Class and the alternative state specific classes. The special relationship arose because financial institutions entrusted Home Depot with customer PII from payment cards they issued. Only Home Depot was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

209. Home Depot's duty to use reasonable data security measures also

arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by retailers such as Home Depot. The FTC publications and data security breach orders described above further form the basis of Home Depot's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

210. Home Depot's duty to use reasonable care in protecting PII arose not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

211. Home Depot breached its common law, statutory and other duties -- and thus was negligent -- by failing to use reasonable measures to protect its customers' personal and financial information from the hackers who perpetrated the 2014 data breach and by failing to provide timely notice of the breach. The specific negligent acts and omissions committed by Home Depot include, but are not limited to, the following:

a. failure to delete cardholder information after the time period necessary to authorize the transaction;

b. failure to employ systems to protect against malware;

c. failure to regularly update its antivirus software;

d. failure to maintain an adequate firewall;

e. failure to track and monitor access to its network and cardholder data;

f. failure to limit access to those with a valid purpose;

g. failure to encrypt PII at the point-of sale;

h. failure to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;

i. failure to assign a unique ID to each individual with access to its systems;

j. failure to automate the assessment of technical controls and security configuration standards;

k. failure to adequately staff and fund its data security operation;

l. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations;

m. failure to heed warnings about specific vulnerabilities in its systems identified by Home Depot's own employees, consultants, and software vendors;

n. failure to recognize red flags signaling that Home Depot's systems

were inadequate and that as a result the potential for a massive data breach akin to the one involving Target was increasingly likely;

o. failure to recognize for approximately five months that hackers were stealing PII from its network while the data breach was taking place;

p. decisions to shelve ongoing projects designed to fix vulnerabilities on its network, including specifically the project to encrypt PII at the point-of-sale; and,

q. failure to disclose the data breach in a timely manner.

212. In connection with the conduct described above, Home Depot acted wantonly, recklessly, and with complete disregard for the consequences.

213. The individuals at Home Depot who committed negligent acts and omissions include those specifically named in this complaint, the company's officers and directors, and others who are not named.

214. As a direct and proximate result of Home Depot's negligence, the Financial Institution Plaintiffs, the FI National Class and the alternative state specific classes have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on

potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

215. Because no statutes of other states are implicated, Georgia common law applies to the negligence claim of the FI National Class. However, if the FI National Class is not certified, the negligence claims of the alternative state specific classes would be governed by the law of each state in which such claims are brought, including applicable statutes relating to data security and notification.

COUNT II
Negligence *Per Se*
On Behalf of the FI National Class and
the Alternative State Specific Classes

216. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by retailers such as Home Depot of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form the basis of Home Depot's duty.

217. Home Depot violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with applicable industry standards, including PCI DSS as described in detail

previously in this complaint. Home Depot's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach at a national retailer, including specifically the immense damages that would result to consumers and financial institutions.

218. Home Depot's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se.*

219. The Financial Intuition Plaintiffs, the FI National Class and the alternative state specific classes are within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, many of the Financial Institution Plaintiffs and absent class members are credit unions, which are organized as cooperatives whose members are consumers.

220. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by the Financial Institution Plaintiffs, the FI National Class and the alternative state specific classes.

221. As a direct and proximate result of Home Depot's negligence *per se*, the Financial Institution Plaintiffs, the FI National Class and the alternative state specific classes have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

222. Because no statutes of other states are implicated, Georgia common law applies to the negligence *per se* claim of the FI National Class. However, if the FI National Class is not certified, the negligence *per se* claims of the alternative state specific classes would be governed by the law of each state in which such state specific claims are brought, including any applicable statutes relating to data security and notification.

COUNT III
Violation of Alaska Unfair Trade Practices and Consumer Protection Act On Behalf of the Alaska Subclass

223. The Alaska Unfair Trade Practices and Consumer Protection Act,

Alaska Stat. § 45.50.471, *et seq.* prohibits unfair methods of competition and unfair practices in the conduct of trade or commerce. Under the express provisions of the Alaska Unfair Trade Practices and Consumer Protection Act, "due consideration and great weight" should be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. *See* Alaska Stat. § 45.50.545.

224. Home Depot engaged in unfair business practices in violation of the Alaska Unfair Trade Practices and Consumer Protection Act by, among other things, failing to implement and maintain reasonable security measures to protect PII and violating industry standards, including PCI DSS.

225. Home Depot's unreasonable failure to implement and maintain reasonable security measures and its violation of industry standards offends public policy as established by statutes, the common law or otherwise and is within at least the penumbra of some common law, statutory or other established concept of unfairness; is immoral, unethical, oppressive, or unscrupulous; and causes substantial injury to consumers, competitors or other businesses,

226. Home Depot failed to spend adequate time and money on its data security practices while Home Depot's competitors spent the resources necessary to safeguard PII in their possession. As a result, Home Depot's conduct not only harmed the members of the Alaska Subclass and those Financial Institution

Plaintiffs with operations in Alaska, but also unfairly harmed competition.

227. Home Depot's practice of maintaining inadequate data security measures provided no benefit to consumers or competition. Accordingly, the substantial injuries sustained by members of the Alaska Subclass and those Financial Institution Plaintiffs with operations in Alaska are not outweighed by any countervailing benefits to consumers or competition. Further, because Home Depot is solely responsible for securing its customer data, there is no way that members of the Alaska Subclass and those Financial Institution Plaintiffs with operations in Alaska could have known about Home Depot's inadequate security practices or avoided their injuries.

228. As a direct and proximate result of Home Depot's unfair and unlawful practices, members of the Alaska Subclass and those Financial Institution Plaintiffs with operations in Alaska have suffered and will continue to suffer injury and ascertainable losses of money and property and thus are entitled to damages in an amount to be proven at trial, three times actual damages, costs and reasonable attorneys' fees, and such other relief as this Court considers necessary and proper.

COUNT IV
Violation of California's Unfair Competition Law And Customer Records Act On Behalf of the California Subclass

229. California Civil Code § 1798.81.5(b) (the "California Customer

Records Act") requires a business that owns, licenses or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

230. Home Depot failed to implement and maintain such reasonable security procedures and practices before and at the time of the 2014 data breach. As a result, Home Depot violated the California Customer Records Act, Cal. Civ. Code § 1798.81.5(b).

231. Further, the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*., ("UCL"), prohibits acts of "unfair competition," which include any "unfair" or "unlawful" business practice.

232. Home Depot engaged in unfair and unlawful business practices prohibited by the UCL by unreasonably failing to adopt and maintain adequate data security measures to protect the personal and financial data of its customers. These unfair and unlawful practices occurred repeatedly in connection with Home Depot's trade or business.

233. Home Depot's failure to adopt and maintain reasonable security measures is unfair within the meaning of the UCL because it constituted an

immoral, unethical, oppressive, and unscrupulous activity; caused substantial injury to consumers and businesses; and provided no benefit to consumers or competition.

234. Home Depot's failure also was unfair within the meaning of the UCL because its conduct undermined California public policy that businesses protect PII as reflected in Article I, Section 1 of the California Constitution (enacted because of private sector data processing activity and stating that all people have an inalienable right to privacy) and in statutes such as the Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22578 (explaining that the Legislature's intent was to have a uniform policy state-wide regarding privacy policies on the Internet); the Information Practices Act, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); and California Civil Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected.").

235. Home Depot's violations of the California Customer Records Act, Cal. Civ. Code § 1798.81.5(b), moreover, constitute unlawful acts or practices under the UCL.

236. The California Subclass and those Financial Institution Plaintiffs operating in California reasonably expected Home Depot to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect their cardholders' personal and financial information.

237. Home Depot's conduct harmed competition. While Home Depot cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by the California Subclass and those Financial Institution Plaintiffs operating in California are not outweighed by any countervailing benefits to consumers or competition. And, because Home Depot is solely responsible for securing its customers PII, there is no way the California Subclass and the Financial Institution Plaintiffs operating in California could have known about Home Depot's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Home Depot's legitimate business interests, other than its conduct responsible for the data breach.

238. As a direct and proximate result of Home Depot's unfair and unlawful practices and violation of UCL and the California Customer Records Act, members of the California Subclass and those Financial Institution Plaintiffs operating in California have suffered and will continue to suffer substantial injury and

ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

COUNT V
Violation of Connecticut Unfair Trade Practices Act
On Behalf of the Connecticut Subclass

239. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110a *et seq.*, prohibits unfair methods of competition and unfair practices in the conduct of trade or commerce. The Connecticut Unfair Trade Practices Act expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. *See* Conn. Gen. Stat. § 42-110b(b).

240. Home Depot engaged in unfair business practices in violation of the Connecticut Unfair Trade Practices Act by, among other things, failing to implement and maintain reasonable security measures to protect its customers' PII, violating industry standards including PCI DSS, and committing the other acts and omissions detailed in this complaint.

241. Home Depot's conduct offends public policy as established by statutes, the common law or otherwise and is within at least the penumbra of some common law, statutory or other established concepts of unfairness; is immoral, unethical, oppressive, or unscrupulous; and causes substantial injury to consumers,

competitors or other businesses.

242. Home Depot's conduct caused substantial injury to Savings Institute and members of the Connecticut Subclass. Home Depot's conduct also harmed competition. While Home Depot cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded.

243. Savings Institute and members of the Connecticut Subclass reasonably expected Home Depot to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect and as necessary delete its customers' private personal and financial information.

244. As a direct and proximate result of Home Depot's unfair and unlawful practices, Savings Institute and members of the Connecticut Subclass have suffered and will continue to suffer injury and ascertainable losses of money and property and thus are entitled to damages in an amount to be proven at trial, costs and reasonable attorneys' fees, and such equitable relief as the Court deems necessary and proper, including injunctive relief.

COUNT VI
Violation of Florida Deceptive and Unfair Trade Practices Act
On Behalf of the Florida Subclass

245. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann.

§ 501.204, ("FDUTPA"), prohibits unfair acts or practices in the conduct of trade or commerce. An "unfair practice" within the meaning of FDUTPA is one that offends established public policy or is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers. Violations of "[t]he standards of unfairness and deception set forth and interpreted by the Federal Trade Commission" also violate FDUTPA. *See* Fla. Stat. Ann. § 501.203(3)(b).

246. Home Depot violated FDUTPA by, among other things, failing to implement and maintain reasonable security measures to protect its customers' PII, not complying with industry standards including PCI DSS, and committing the other acts and omissions detailed in this complaint.

247. Although no injury is required to obtain relief under FDUTPA, Suncoast and members of the Florida Subclass have suffered and will continue to suffer injury as a direct and proximate result of Home Depot's unfair and unlawful practices prohibited by the statute. As a result, Suncoast and members of the Florida Subclass are entitled to damages in an amount to be proven at trial, reasonable attorneys' fees, costs, and injunctive relief.

COUNT VII
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act On Behalf of the Illinois Subclass

248. The Illinois Consumer Fraud and Deceptive Business Practices Act,

815 Ill. Comp. Stat. 505/1, *et seq.*, prohibits unfair acts or practices. In determining whether an act or practice is unfair, the Act expressly requires that consideration be given to interpretations of the FTC relating to Section 5 of the Federal Trade Commission Act. *See* 815 Ill. Comp. Stat. 505/2.

249. Home Depot engaged in unfair business practices in violation of the Illinois Consumer Fraud and Deceptive Business Practices Act by failing to implement and maintain reasonable security measures, violating industry standards such as PCI DSS, and committing the other acts and omissions detailed in this complaint.

250. Home Depot's conduct offends public policy; is immoral, unethical, oppressive, or unscrupulous; and caused substantial injury to consumers, competitors or other businesses.

251. Home Depot's conduct specifically caused substantial injury to members of the Illinois Subclass and those Financial Institution Plaintiffs operating in Illinois. Home Depot's conduct also harmed competition. While Home Depot cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded.

252. Members of the Illinois Subclass and those Financial Institution

Plaintiffs operating in Illinois reasonably expected Home Depot to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect and as necessary delete its customers' PII.

253. Home Depot's practice of maintaining inadequate data security measures provided no benefit to consumers or competition. Accordingly, the substantial injuries sustained by the Illinois Subclass and those Financial Institution Plaintiffs operating in Illinois are not outweighed by any countervailing benefits to consumers or competition. Further, because Home Depot is responsible for securing its customer data, members of the Illinois Subclass and those Financial Institution Plaintiffs operating in Illinois could not have known about Home Depot's inadequate security practices or avoided their injuries.

254. As a direct and proximate result of Home Depot's unfair and unlawful practices, members of the Illinois Subclass and those Financial Institution Plaintiffs operating in Illinois have suffered and will continue to suffer injury and are entitled to damages in an amount to be proven at trial, reasonable attorneys' fees and costs, and injunctive relief.

COUNT VIII
Violation of the Massachusetts Consumer Protection Act
On Behalf of the Massachusetts Subclass

255. The Massachusetts Consumer Protection Act, Mass. Gen. Laws. Ch.

93A, *et seq.*, makes it unlawful to engage in any "unfair or deceptive acts or practices in the conduct of any trade or commerce" and, in interpreting its provisions, requires express consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. *See* Mass. Gen. Laws. Ch. 93A § 2(b).

256. Home Depot violated the Massachusetts Consumer Protection Act, Mass. Gen. Laws Ch. 93A §§ 2 and 11, by failing to implement and maintain reasonable security measures, violating industry standards such as PCI DSS, and committing the other acts and omissions detailed in this complaint.

257. Home Depot's conduct offends public policy as established by statutes, the common law or otherwise and is within at least the penumbra of some common law, statutory or other established concept of unfairness; is immoral, unethical, oppressive, or unscrupulous; and caused substantial injury to consumers, competitors or other businesses.

258. Home Depot's conduct provided no benefit to consumers or competition. Accordingly, the substantial injuries sustained by the Massachusetts Subclass and those Financial Institution Plaintiffs operating in Massachusetts are not outweighed by any countervailing benefits to consumers or competition. Further, because Home Depot is responsible for securing its customer data,

members of the Massachusetts Subclass and those Financial Institution Plaintiffs operating in Massachusetts could not have known about Home Depot's inadequate security practices or avoided their injuries.

259. The actions and transactions constituting Home Depot's unfair acts and practices under this claim occurred primarily and substantially in Massachusetts under the pragmatic, functional analysis employed by courts because: (a) Home Depot's unlawful conduct was intended to and did impact payment card transactions in its stores, approximately forty-five in number, located in Massachusetts; (b) members of the Massachusetts Subclass were located in Massachusetts and incurred losses and suffered damages there; (c) payment cards used by Massachusetts consumers were stolen at stores located there and the stolen information was used to commit fraud in Massachusetts; and (d) Home Depot's unlawful conduct interfered with trade or commerce in Massachusetts.

260. As a direct and proximate result of Home Depot's unfair and unlawful practices, the Massachusetts Subclass and those Financial Institution Plaintiffs operating in Massachusetts have suffered and will continue to suffer ascertainable loss of money and property and thus are entitled to damages in an amount to be proven at trial, reasonable attorneys' fees, costs, and such other relief, including injunctive relief, as the Court deems to be necessary and proper.

COUNT IX
Violation of the Minnesota Plastic Card Security Act
On Behalf of the Minnesota Subclass

261. The Minnesota Plastic Card Security Act, Minn. Stat. §325E.64, imposes a duty on merchants conducting business in Minnesota to safeguard payment card data obtained from their customers by deleting such data immediately after authorization of a credit card transaction or, in the case of a PIN debit transaction, within 48 hours after authorization of the transaction. A private right of action is expressly provided to those injured by a violation of the statute.

262. Specifically, Minn. Stat. § 325E.64, subdivision 2 provides:

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

263. Home Depot, which operates approximately 33 stores in the state, conducts business in Minnesota.

264. Home Depot regularly accepts debit and credit cards, which are "access devices" within the meaning of the statute, in connection with sales transactions and for the purpose of conducting business in Minnesota.

265. Home Depot violated the Minnesota Plastic Card Security Act by retaining payment card data (the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data) longer than allowed by the statute – i.e., subsequent to the authorization of the transaction or, in the case of a PIN debit transaction, subsequent to 48 hours after authorization.

266. As a direct and proximate result of Home Depot's violation of the Minnesota Plastic Card Security Act, Profinium and members of the Minnesota Subclass have suffered and will continue to suffer damage, including the costs specifically set forth in Minn. Stat. § 325E.64, and thus are entitled to damages in an amount to be proven at trial.

COUNT X
Violation of Wash. Rev. Code § 19.255.020
On Behalf of the Washington Subclass

267. The Washington Legislature, in an effort to combat cybercrime and to protect financial institutions from negligent practices of retailers, enacted Wash. Rev. Code § 19.255.020, which states in pertinent part:

> If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in

> the state of Washington as a consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach.

268. Sound Community and members of the Washington Subclass are "financial institutions" within the meaning of Wash. Rev. Code § 19.255.020.

269. Defendants are "business[es]" within the meaning of Wash. Rev. Code § 19.255.020.

270. The information compromised in the 2014 data breach at Home Depot was "account information" within the meaning of Wash. Rev. Code § 19.255.020.

271. Home Depot violated Wash. Rev. Code § 19.255.020 by failing to implement and maintain reasonable security measures, violating industry standards, and committing the other acts and omissions detailed in this complaint.

272. As a direct and proximate result of Home Depot's violation of Wash. Rev. Code § 19.255.020, Sound Community and members of the Washington Subclass have been damaged and thus are entitled to recover the reasonable and actual costs they incurred in reissuing compromised payment cards and mitigating injuries to their cardholders who reside in Washington resulting from the breach.

COUNT XI
Violation of Wash. Rev. Code § 19.86.010, *et seq.*
On Behalf of the Washington Subclass

273. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86,

et seq., prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.

274. Under the Washington Consumer Protection Act, a claim may be founded on, among other things, a *per se* violation of a statute or an unfair (or deceptive) practice unregulated by statute but involving the public interest.

275. Home Depot violated Wash. Rev. Code § 19.255.020(3)(a) as set forth above and thereby committed a *per se* violation of the Washington Consumer Protection Act, Wash. Rev. Code § 19.86, *et seq.*

276. Members of the Washington Subclass and those Financial Institution Plaintiffs operating in Washington are within the class of persons Wash. Rev. Code § 19.255.020 seeks to protect.

277. As a result of Home Depot's *per se* violations of the Washington Consumer Protection Act, the Washington Subclass and those Financial Institution Plaintiffs operating in Washington have been injured in their business and property, suffered monetary damages, and thus are entitled to actual damages, three times actual damages, attorneys' fees and costs, and injunctive relief.

COUNT XII
Declaratory and Injunctive Relief
On Behalf of All Plaintiffs

278. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, this

Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described in this complaint.

279. An actual controversy has arisen in the wake of Home Depot's data breach regarding its common law and other duties to reasonably safeguard its customers' PII. Plaintiffs allege that Home Depot' data security measures were inadequate and remain inadequate. Home Depot denies these allegations. Furthermore, Plaintiffs continue to suffer injury as additional fraudulent charges are being made on payment cards they issued to Home Depot customers.

280. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Home Depot owed and continues to owe a legal duty to secure its customers' personal and financial information – specifically including information pertaining to credit and debits cards used by Home Depot's customers – and to notify financial institutions of a data breach under the common law, Section 5 of the FTC Act, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

b. Home Depot breached and continues to breach this legal duty by failing to employ reasonable measure to secure its customers' personal and financial information;

c. Home Depot's breach of its legal duty proximately caused the data breach which occurred between April and September, 2014; and,

d. Banks, credit unions, and other institutions that reissued payment cards and were forced to pay for fraudulent transactions as a result of the Home Depot data breach are legally entitled to recover the costs they incurred from Home Depot.

281. The Court also should issue corresponding injunctive relief requiring Home Depot to employ adequate security protocols consistent with industry standards to protect its customers' personal and financial information. Specifically, this injunction should, among other things, direct Home Depot to:

a. utilize industry standard encryption to encrypt transmission of cardholder data at the point-of-sale and at all other times;

b. implement encryption keys in accordance with industry standards;

c. consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;

d. audit, test, and train its data security personnel regarding any new or

modified procedures and how to respond to a data breach;

e. regularly test its systems for security vulnerabilities, consistent with industry standards;

f. comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information;

g. install all upgrades recommended by manufacturers of security software and firewalls used by Home Depot; and

h. delete customers' credit card information immediately after obtaining authorization to process the transaction and, as to PIN debit transactions, no later than 48 hours after authorization of the transaction, as required by the Minnesota Plastic Card Security Act.

282. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Home Depot. The risk of another such breach is real, immediate, and substantial. If another breach at Home Depot occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

283. The hardship to the Financial Institution Plaintiffs and absent class members if an injunction does not issue exceeds the hardship to Home Depot if an

injunction is issued. Among other things, if another massive data breach occurs at Home Depot, the Financial Institution Plaintiffs and absent class members will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Home Depot of complying with an injunction by employing reasonable data security measures is relatively minimal, and Home Depot has a pre-existing legal obligation to employ such measures.

284. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Home Depot, thus eliminating the injuries that would result to Plaintiffs and the millions of consumers whose confidential information would be compromised.

285. The Association Plaintiffs are participating in this lawsuit on behalf of their members. They seek, where their members are entitled to do so and the claims for relief otherwise permit, the declaratory and injunctive relief requested above on behalf of their members who will continue to suffer as a result of Home Depot's conduct unless it is stopped.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the classes, respectfully request that the Court:

a. Certify the classes and appoint Plaintiffs and Plaintiffs' counsel to represent the classes;

b. Enter a money judgment in favor of the Financial Institution Plaintiffs and members of the classes to compensate them for the injuries they have suffered together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

c. Enter a declaratory judgment in favor of all Plaintiffs as described above;

d. Grant Plaintiffs the injunctive relief they have requested;

e. Award Plaintiffs and the classes reasonable attorneys' fees and costs of suit, including specifically fees and expenses under O.C.G.A. § 13-6-11 on the ground that Home Depot has acted in bad faith, has been stubbornly litigious, and caused unnecessary trouble and expense within the meaning of that statute; and,

f. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all claims so triable.

/s/ *Kenneth S. Canfield*
Kenneth S. Canfield
Georgia Bar No. 107744
DOFFERMYRE SHIELDS
CANFIELD & KNOWLES, LLC
1355 Peachtree St., NE, Suite 1600
Atlanta, Georgia 30309-3238
Telephone: 404-881-8900
kcanfield@dsckd.com
Co-lead Counsel

Joseph P. Guglielmo
SCOTT & SCOTT, LLP
405 Lexington Avenue
New York, New York 10174
Telephone: 212-594-5300
jguglielmo@scott-scott.com
Co-lead Counsel

Gary F. Lynch
CARLSON LYNCH SWEET
& KILPELA, LLP
PNC Park, Suite 210
115 Federal Street
Pittsburgh, Pennsylvania 15212
Telephone: 412-322-9343
glynch@carlsonlynch.com
Co-lead Counsel

W. Pitts Carr
W. PITTS CARR AND
ASSOCIATES, PC
4200 Northside Parkway, NW
Building 10
Atlanta, Georgia 30327
Telephone: 404-442-9000
pcarr@wpcarr.com
Co-liaison Counsel

Ranse M. Partin
CONLEY GRIGGS PARTIN,
LLP
1380 West Paces Ferry Road, NW
Suite 2100
Atlanta, Georgia 30327
Telephone: 404-467-1155
ranse@conleygriggs.com
Co-liaison Counsel

Plaintiffs' Steering Committee

James H. Pizzirusso
HAUSFELD, LLP
1700 K. Street, NW, Suite 650
Washington, DC 20006
Telephone: 859-225-3731
jpizzirusso@hausfeldllp.com
Plaintiffs' Steering Committee Chair

Robert N. Kaplan
KAPLAN FOX & KILSHEIMER
850 Third Ave., 14th Floor
New York, New York 10022
Telephone: 212-687-1980
rkaplan@kaplanfox.com

Joseph Hank Bates, III
CARNEY BATES & PULLIAM
17 Washington Ave., N., Suite 300
Minneapolis, MN 55401
Telephone: 501-312-8500
jbates@cbplaw.com

W. Daniel Miles, III
Andrew E. Brasher
Leslie L. Pescia
BEASLEY ALLEN CROW
MEHTVIN PORTIS & MILES
P.O. Box 4160
218 Commerce Street
Montgomery, Alabama 36103
Telephone: 334-269-2343
Dee.Miles@beasleyallen.com

Bryan L. Bleichner
Chestnut Cambronne, PA
17 Washington Avenue North
Suite 300
Minneapolis, MN 55401
Telephone: 612-339-7300
bbleichner@chestcambronne.com

Arthur M. Murray
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, Louisiana 71030
Telephone: 505-525-8100
amurray@murray-lawfirm.com

Brian C. Gudmundson
ZIMMERMAN REED, PLLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55042
Telephone: 612-341-0400
Brian.gudmundson@zimmreed.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN
100 Washington Ave., So., Suite 2200
Minneapolis, MN 55401
Telephone: 612-339-6900
khriebel@locklaw.com

Vincent J. Esades
David R. Woodward
HEINS MILLS & OLSON, PLC
310 Clifton Avenue
Minneapolis, MN 55403
Telephone: 612-338-4605
vesades@heinsmills.com

Thomas A. Withers
GILLEN WITHERS & LAKE
8 E. Liberty Street
Savannah, Georgia 31401
Telephone: 912-447-8400
twithers@gwllawfirm.com

Andrew N. Friedman
COHEN MILLSTEIN SELLERS TOLL
1100 New York Ave., NW
East Tower, 5th Floor
Washington, DC 20005
Telephone 202-408-4600
afriedman@cohenmilstein.com

Counsel for the Financial Institution Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on May 27, 2015, I served all parties by causing a true and correct copy of the foregoing Financial Institution Plaintiffs' Consolidated Class Action Complaint to be filed with clerk of court using the CM/ECF system, which automatically sends a copy to all counsel registered to receive service.

/s/ *Kenneth S. Canfield* .
Kenneth S. Canfield

Co-Lead Counsel for the
Financial Institution Plaintiffs