IN THE UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

MARY LOU BENNEK,

Plaintiff,

v.

F. DUANE ACKERMAN, ARI BOUSBIB, GREGORY D. BRENNEMAN, J. FRANK BROWN, ALBERT P. CAREY, ARMANDO CODINA, HELENA B. FOULKES, KAREN L. KATEN, CRAIG A. MENEAR, MARK VADON, FRANCIS S. BLAKE, TERESA WYN ROSEBOROUGH,

Defendants,

and

THE HOME DEPOT, INC.,

Nominal Defendant.

NO. 1:15-CV-2999

VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT

[FILED CONDITIONALLY UNDER SEAL - CONFIDENTIAL]

1. Plaintiff Mary Lou Bennek ("Bennek" or "Plaintiff") brings this shareholder derivative case after the actions and conscious inaction of officers and directors of The Home Depot, Inc. ("Home Depot" or the "Company") resulted in one of the largest data breaches in U.S. history. Plaintiff asserts claims derivatively on behalf of Home Depot for breach of



Redacted

fiduciary duty and waste of corporate assets against certain current and former Company officers and directors.

## NATURE OF THE CLAIMS

2. Throughout the period January 1, 2011 through September 8, 2014 (the "Relevant Period"), [redacted] Home Depot was not employing reasonable measures to protect its customers' personal and financial information, including by maintaining its computer systems in accordance with Payment Card Industry Data Security Standards ("PCI DSS") as required by its contracts with payment card processors and networks, including Visa and MasterCard.

3. During the Relevant Period, Matthew Carey, Home Depot's Executive Vice President and Chief Information Officer, reported directly to Frank Blake, Home Depot's CEO, [redacted]

4. Ironically, the remedies for many of Home Depot's computer system's vulnerabilities were already at hand and required only commitment by Individual Defendants to ensure that they were implemented in a timely manner. But instead of acting immediately to remedy a system that its own CEO, Frank Blake, characterized as being "desperately out of date," the Individual Defendants were complacent, leaving in place glaring vulnerabilities that not only allowed hackers to enter the system undetected but permitted them to continue siphoning customer cardholder and personal data for almost five months without detection.



Redacted

5. Between April and September 2014, Home Depot's "desperately out of date" data security system was subject to one of the largest retail data breaches in our nation's history (the "Data Breach" or the "Breach"). Hackers stole the personal and financial information of approximately 56 million Home Depot customers, and that information was then sold on the Internet to others so that they could in turn commit debit and credit card fraud.

[redacted]

7. Following the Breach, consumers and financial institutions filed at least 44 civil actions against Home Depot, claiming that Home Depot failed to implement reasonable measures to prevent or mitigate the effects of the Data Breach. Central to the allegations in these lawsuits is the claim that Home Depot failed to honor its contractual obligations to abide by PCI DSS, which establishes a minimum level of data security for consumer debit and credit card transactions. The total losses for all financial institutions due to the Data Breach have been estimated in the billions of dollars.

8. Plaintiff now brings suit derivatively on Home Depot's behalf to remedy the Individual Defendants' breaches of their fiduciary duties of loyalty, good faith, and due care by knowingly and in conscious disregard of their duties failing to ensure that Home Depot took reasonable measures to protect its customers' personal and financial information.

9. In addition to seeking monetary relief for the damages suffered by Home Depot, Plaintiff also seeks improvements to the Company's corporate governance structure, which will help restore consumers' and financial institutions' confidence in Home Depot's ability to protect its customers' sensitive personal and financial information in the future.

## JURISDICTION AND VENUE

10. Jurisdiction is conferred by 28 U.S.C. §1332. Complete diversity among the parties exists, and the amount in controversy exceeds $75,000, exclusive of interest and costs.



Redacted

11. This Court has jurisdiction over each defendant named herein because each defendant is either a corporation that conducts business in and maintains operations in this District or is an individual who has sufficient minimum contacts with this District to render the exercise of jurisdiction by the District Court permissible under traditional notions of fair play and substantial justice.

12. Venue is proper in this Court in accordance with 28 U.S.C. §1391(a) because: (i) Home Depot maintains its principal place of business in this District; (ii) one or more of the defendants either resides in or maintains executive offices in this District; (iii) a substantial portion of the transactions and wrongs complained of herein, including the Individual Defendants' primary participation in the wrongful acts detailed herein, and aiding and abetting and conspiracy in violation of fiduciary duties owed to Home Depot, occurred in this District; and (iv) the Individual Defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

## THE PARTIES

***Plaintiffs***

13. Plaintiff Mary Lou Bennek ("Plaintiff" or "Bennek") has held shares of Home Depot stock continuously since at least 2003 and is a current Home Depot shareholder. Bennek is a citizen of Arizona.

***Nominal defendant***

14. The Home Depot, Inc. is a Delaware corporation with principal executive offices located at 2455 Paces Ferry Road, N.W., Atlanta, Georgia 30339. Home Depot is a citizen of Georgia. Home Depot describes itself as the world's largest home improvement retailer, with stores in numerous countries, and the fourth largest retailer in the United States. It sells a wide assortment of building materials, home improvement and lawn and garden products, home appliances, plumbing and electrical supplies, and provides a number of related services.

***Defendants***

15. F. Duane Ackerman ("Ackerman") was a member of Home Depot's Board of Directors from January 1, 2007 through May 21, 2015. He served on Home Depot's Audit Committee throughout the Relevant Period. Ackerman is a citizen of Georgia.

16. Ari Bousbib ("Bousbid") has been a member of Home Depot's Board of Directors since 2007. Bousbib was a member of the Board's Audit Committee during the Relevant Period. Bousbib is a citizen of Connecticut.

17. Gregory D. Brenneman ("Brenneman") has been a member of Home Depot's Board of Directors since 2000. Brenneman is a citizen of Texas.

18. J. Frank Brown ("Brown) has been a member of Home Depot's Board of Directors since 2011. Brown was a member of the Board's Audit Committee during the Relevant Period. Brown is a citizen of New York.

19. Albert P. Carey ("Albert Carey") has been a member of Home Depot's Board of Directors since 2008. Albert Carey is a citizen of New York.

20. Armando Codina ("Codina") has been a member of Home Depot's Board of Directors since 2007. Codina is a citizen of Florida.

21. Helena B. Foulkes ("Foulkes") has been a member of Home Depot's Board of Directors since 2013. Foulkes is a citizen of Rhode Island.

22. Karen L. Katen ("Katen") has been a member of Home Depot's Board of Directors since 2007. Katen was a member of the Board's Audit Committee during the Relevant Period. Katen is a citizen of California.

23. Craig A. Menear ("Menear") has been Home Depot's CEO and President since November 1, 2014, and has been Chairman of the Board since February 2, 2015. Menear was Home Depot's President, U.S. Retail from February 2014 to October 2014. From 2007 to February 2014, Menear was Home Depot's Executive Vice President of Merchandising. Menear is a citizen of Georgia.

24. Mark Vadon ("Vadon") has been a member of Home Depot's Board of Directors since 2012. Vadon was a member of the Board's Audit Committee during the Relevant Period. Vadon is a citizen of Washington.

25. Francis S. Blake ("Blake) was Home Depot's CEO and Chairman of the Board during the period January 2007 to November 1, 2014. Blake remained as Home Depot's Chairman of the Board until February 2, 2015. Blake is a citizen of Georgia.

26. Teresa Wyn Roseborough ("Roseborough") has served as Home Depot's executive vice president, general counsel and corporate secretary since October 2011. Roseborough has been responsible for all corporate governance matters and legal functions at Home Depot since October 2011. Roseborough is a citizen of Georgia.

27. Collectively, the defendants identified in ¶¶15-26 are referred to herein as the "Individual Defendants."

## WRONGDOING

***The Individual Defendants Knew that the Risk of Loss of a Substantial Amount of Customer Data Presented a Top Ten Enterprise Risk to Home Depot and They Knew That Home Depot's Computer Systems Were Vulnerable to Hackers Who Were Likely to Target the Retail Giant.***

28. During the Relevant Period, the Individual Defendants were well-aware that a data security breach such as the one that occurred from April to September 2014 was a substantial "Risk Factor" for the Company.

29. As early as 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 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.

[redacted]

***The Individual Defendants Knew That Home Depot Was Not Implementing Reasonable Measures to Secure Its Customers' Data, Including Measures That Were Required by Its Contracts with the Payment Card Industry.***

31. Prior to and during the time that the Data Breach occurred,

Home Depot was required, pursuant to its agreements with payment card processors and networks, including Visa and MasterCard, to abide by PCI DSS to protect its customers' personal and financial data. PCI DSS applies to all organizations that store, process, or transmit payment card data. PCI DSS establishes the minimum level of protection required, not the maximum.

32. PCI DSS 3.0, the version of the standards in effect at the time of the Data Breach, required that Home Depot:

a. install and maintain a firewall configuration to prevent unauthorized access to Home Depot's systems upon which cardholder data is transmitted and stored;

b. protect all systems against malware and regularly update anti-virus software or programs so as to thwart any unauthorized persons who are able to gain access to Home Depot's systems;

c. not store such data beyond the time necessary to authorize a transaction and encrypt cardholder data that is transmitted and stored on Home Depot's systems so as to render that data unreadable to unauthorized persons;

d. limit access to payment card data to those with a need to know and track and monitor all access to cardholder data, including by assigning unique identification numbers to each individual with access to its systems; and



Redacted

e. regularly test its data security systems and processes so as to be able to effectively prevent or detect and address any unauthorized access to cardholder data in a timely manner.

[redacted]

34. 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."

35. If the Individual Defendants had ensured that Home Depot abided by its contractual obligations to comply with the PCI DSS standards, the Data Breach and the damages resulting therefrom could have been avoided entirely or substantially mitigated.

***The Individual Defendants Failed to Ensure That Home Depot Installed and Maintained an Adequate Firewall.***

36. Throughout the Relevant Period, the PCI DSS required retailers to install and maintain an adequate firewall in order to prevent unauthorized persons from gaining access to systems upon which cardholder data was transmitted or stored.

37. A firewall is a network security system, either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules. Acting as a barrier between a trusted network and other untrusted networks (e.g., the Internet) or less-trusted networks (e.g., a retail merchant's network outside of a cardholder data environment), a firewall controls access to the resources of a network through a positive control model. This means that only traffic expressly allowed in the firewall policy is permitted onto the network; all other traffic is denied.

38. Prior to and during the time of the Data Breach, Home Depot used computer security software made by Symantec Corporation ("Symantec") known as "Endpoint Protection 11.0." Endpoint Protection provided three primary security features: (1) a client firewall



Redacted

("Network Threat Protection" or "NTP"); (2) behavior-based threat protection ("Proactive Threat Protection"); and (3) antivirus and antispyware tools.

39. However, Home Depot disabled Endpoint Protection's NTP firewall. According to Symantec, NTP "blocks threats from accessing your computer by using rules and signatures." This left Home Depot vulnerable to intruders freely accessing their internal network.

40. In Symantec's documentation for configuring Endpoint Protection 11.0, Symantec warns customers, "Firewalls are only as good as the policies they enforce. A poorly constructed policy can effectively let attackers in while preventing trusted sources from accessing necessary resources. Before you configure the client firewall, you should understand how the firewall processes rules, how to create rules effectively (protect while maximizing performance), and how the firewall interacts with the other components of Symantec Endpoint Protection."

41. Despite these warnings, Home Depot turned off the the NTP client firewall and instead solely relied upon older Windows software that was considered antiquated and ineffective for firewall protection at the time.

42. During the Relevant Period, Matthew Carey served as Home Depot's Chief Information Officer and reported directly to Home Depot's CEO, Frank Blake. [redacted] Matthew Carey's principal deputy responsible for data security was Jeff Mitchell. Mitchell 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 at Home Depot. [redacted]

43. Since at least 2011, Home Depot's IT employees had warned Mitchell and Carey that use of the built-in Windows firewall rendered Home Depot's computer systems vulnerable to hackers and recommended that Home Depot activate the NTP firewall.



Redacted

[redacted]

45. In August 2013, Visa sent a letter to Home Depot entitled "Retail Merchants Targeted by Memory-Parsing Malware." The letter warned Home Depot that, since January 2013, Visa had seen an increase in network intrusions involving retail merchants using Windows based cash register systems.

46. Visa's warning echoed the warnings that Home Depot's IT personnel had provided to Matthew Carey and Mitchell since 2011 regarding the weakness of Home Depot's Windows based firewall.

47. On October 1, 2013, IT security consultant FishNet Security issued a report to Home Depot, warning that the Company was leaving its computers vulnerable because it had switched off Symantec's NTP firewall in favor of the Windows firewall. The report stated, "It is highly advised and recommended the NTP Firewall component be deployed and that Windows Firewall be discontinued." The FishNet report further stated that "NTP was needed on all Home Depot computers, including register payment terminals," in order for the Company's intrusion prevention system to work properly. Notwithstanding that FishNet's report reiterated Visa's earlier warning about the inadequacy of Home Depot's Windows-based firewall, Home Depot continued to rely solely on the built-in Windows firewall and failed to activate the more secure Symantec NTP firewall.

48. Further warnings regarding the need to deploy the NTP firewall, and to cease relying upon the flawed Windows firewall, were provided in late 2013, when retailers, including Target and Neiman Marcus, suffered a series of data breaches by hackers that took advantage of the flawed Windows firewall.



Redacted

49. [redacted] Nonetheless, as of April 2014, according to reports by former Home Depot security personnel, Home Depot was still relying solely upon the Windows firewall and had not deployed the NTP firewall. Given that the Company possessed the more secure Symantec software, Home Depot's decision to actively not enable the NTP failure was inexplicable.

***The Individual Defendants Failed to Ensure That Home Depot Encrypted Cardholder Data That Was Transmitted and Stored on Its Systems.***

50. Throughout the Relevant Period, PCI DSS also mandated that retailers not store cardholder data any longer than necessary and encrypt any cardholder data at the point of sale so as to render any retained data unreadable to hackers. PCI DSS explained that, even if an intruder was able to penetrate the firewall, encryption at the point of sale could still protect the data accessed and thereby reduce the risk of loss.

51. Encryption is a cryptographic process by which data is encoded in such a way that only authorized parties can decrypt it. Without the proper private key, encrypted information appears as a string of undecipherable characters. Only after after a user unlocks the information with her private key does it transform the data to its original, user-readable form. Encryption is the last, critical defense against cyber attackers and identity thieves.

52. [redacted] Because of the lack of encryption, after a customer's payment card was swiped, the data related to credit and debit card transactions on the card's magnetic stripe would remain visible in clear text (and thus vulnerable to hackers) while being sent from Home Depot's stores to its main servers.

53. Beginning no later than 2009, external consultants warned Home Depot that its failure to encrypt customer data at the point of sale posed a substantial risk. After cards were swiped, the data on the magnetic stripes remained visible in clear text (and thus vulnerable to



Redacted

hackers) while being sent to Home Depot's main servers. In contrast, point of sale encryption would have protected cardholders' data, so that even if it was intercepted while in transit to Home Depot's servers, the card information would have been unreadable by hackers.

54. Home Depot's own internal IT employees repeatedly warned Jeff Mitchell that Home Depot should be encrypting its customers' data at the point of sale. In 2012, frustrated with the lack of action in response to their concerns, the IT employees went over Mitchell's head and spoke directly with Matthew Carey regarding their concerns about data security, and specifically, the need to encrypt customers' data at the point of sale.

55. Despite these warnings, and although Home Depot had the capability of implementing point-of-sale encryption [redacted]

56. By early September 2014, when the Breach was discovered, Home Depot had still failed to install encryption technology at seventy-five percent of its stores.

57. The failure to install the encryption technology promptly was not due to any technological hurdles. Upon learning its network had been breached, Home Depot was able to install the encryption technology at the remaining seventy-five percent of its stores in just eleven days—and had that technology tested and validated by two independent IT security firms.

***The Individual Defendants Failed to Ensure That Home Depot Installed and Maintained Up-to-Date Antivirus and Antispyware Software.***

58. Throughout the Relevant Period, PCI DSS also required that retailers install and maintain up to date antivirus and antispyware software to prevent hackers from installing malware that would enable them to steal customer data.

59. Prior to and during the time of the Data Breach, [redacted] Home Depot was using outdated antivirus and antispyware software that had been released in 2007, the same Symantec product discussed earlier, Endpoint Protection 11.

60. In 2011, Symantec had released a new version of its security software, called Endpoint Protection 12. According to Symantec, Endpoint Protection 12 was needed because



Redacted

the "threat landscape had changed significantly" and the new product would better protect against the "explosion in malware scope and complexity."

61. When Endpoint Protection 12 was released, Home Depot information security managers advised that Endpoint Protection 12 should be installed, because Endpoint Protection 11 was outdated, and Endpoint Protection 12 would substantially improve the Company's antivirus and antispyware protection. However, the Individual Defendants did not ensure that the Company install up to date security software.

62. The Individual Defendants received a warning that hackers were targeting Home Depot and that its outdated antivirus and antispyware software could not prevent their attacks in July 2013. At that time, data stealing malware was placed on at least eight point-of-sale terminals at a Home Depot store in Denton, Texas.

63. In December 2013, the Individual Defendants received another warning. At that time, 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. The incident was yet another signal that hackers might be planning an attack on Home Depot and emphasized the need to update the Company's security software.

64. Nonetheless, Home Depot continued to use the outdated software up to and through the time of the Data Breach.

65. In fact, the 2007 antivirus and antispyware software that Home Depot was using at the time of the Data Breach was so outdated that all support for the product was slated to be terminated on January 5, 2015. In early 2014, Symantec had warned users of Endpoint Protection 11 that "This is the end of the product life cycle."

66. In July 2014, while the Data Breach was ongoing, Home Depot contracted with Symantec to perform a "health check" on its computer systems. The health check identified as critical issues that Home Depot continued to use out-of-date antivirus software and malware detection systems on its point-of-sale terminals.



Redacted

67. Nonetheless, up through the time that the Data Breach was detected, the Individual Defendants failed to ensure that Home Depot installed and maintained up to date antivirus and antispyware software.

***The Individual Defendants Failed to Ensure That Home Depot Properly Limited Access to Payment Card Data to Authorized Persons in Violation of Industry Standards.***

68. Throughout the Relevant Period, PCI DSS also required that retailers limited access to payment card data to those with a need to know and tracked and monitored all access to cardholder data, including by assigning unique identification numbers to each individual with access to its systems.

[redacted]



Redacted

[redacted]

72. Because Home Depot failed to abide by the PCI DSS regarding limiting and monitoring access to its systems, hackers were able to use privileged access granted to one of its vendors to gain access to Home Depot's systems and cardholder data during the Data Breach.

***The Individual Defendants Failed to Ensure That Home Depot Effectively Monitored Its Systems to Prevent and Detect Unauthorized Access to Cardholder Data.***

73. Throughout the Relevant Period, PCI DSS also required that retailers have approved, third-party quality security assessors, using technologies approved by the PCI Security Standards Council, and conduct quarterly scans of their systems for unusual activity, including at point of sale terminals. The purpose of these standards is to enable retailers to detect and mitigate harm caused by unauthorized access to cardholder data in a timely manner.

[redacted]

75. During the 2011-2014 period, Home Depot's own IT employees regularly complained to Matthew Carey and Mitchell that only a small percentage of Home Depot's stores were being scanned for vulnerabilities, and only a small percentage of the computers in those stores were being monitored. Further, the employees warned, the vulnerability scans were only irregularly performed.

76. Home Depot employees explained that Home Depot could have dramatically improved its ability to scan its systems for vulnerabilities by deploying its "Symantec Control Compliance Suite" software. This software would have enabled Home Depot to automate its monitoring processes, allowed its network to be assessed centrally, using consistent standards, and much more frequently. Instead, because the software was not deployed, Home Depot's IT staff had to continue using a tedious, manual process to scan the Company's systems for vulnerabilities that left the network exposed to attack.



Redacted

77. Furthermore, during the 2011-2014 period, Home Depot employees regularly complained to Matthew Carey and Mitchell about the lack of bandwidth on Home Depot's computer network, which prevented them from being able to upload the security logs for the Company's point of sale terminals so that they could be reviewed at corporate headquarters.

[redacted]

***Cyber Attacks on Major Retailers, Including Target and Neiman Marcus, Alerted the Individual Defendants to the Heightened Probability That Home Depot Would Also Be Attacked.***

80. In December 2013, Home Depot 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 the payment card information of 40 million customers and the other personal information of an



Redacted

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.

[redacted]

83. Following the Target and Neiman Marcus data breaches, Home Depot executives, led by then CEO Frank Blake, assembled a task force to begin to devise a plan to prevent a similar attack at Home Depot. Blake requested that Matthew Carey and IT personnel working under his direction 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. Home Depot would ultimately put together a 45-page playbook on 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; and (f) implementing technology to encrypt payment card data on point-of sale terminals. Most of these recommendations mirrored the advice that Home Depot's employees, outside consultants, and vendors had provided to the Company for years.

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

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



Redacted

86. 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 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 security software, activating all of the software's features, replacing the outdated Windows firewall, and encrypting customer data on point-of-sale terminals.

87. On February 13, 2014, in response Home Depot's request that it investigate the Company's exposure to a previously unknown vulnerability in Adobe's Flash Player, data security consultant FishNet advised Home Depot that the firewall protection that it was using was inadequate.

88. At around the same time, because of concern regarding Home Depot's lax approach to data security, three of Symantec's contractors refused to continue working for Home Depot, and Symantec itself threatened to cease doing business with the Company, unless Home Depot began to take security more seriously.

[redacted]



Redacted

[redacted]

90. [redacted]

91. Several months later, in July 2014, while the Data Breach continued undetected, Home Depot contracted with Symantec to perform a "health check" on its computer systems. The health check reiterated prior critical warnings that Home Depot was using out-of-date antivirus software and malware detection systems on its point-of-sale terminals.

[redacted]



Redacted

[redacted]

**Detection of the Data Breach and Its Aftermath**

95. The Individual Defendants' abject failure to fulfill their fiduciary duties to oversee and manage risks at Home Depot related to data security was well evidenced, not only by the ease with which hackers were able to penetrate Home Depot's systems and install malicious code, which enabled them to steal the personal and financial data of millions of Home Depot customers, but also by the length of time that the Breach was allowed to continue undetected. Not only did Home Depot's cybersecurity system fail to deter the Breach in the first place, but it ultimately failed to even detect the Data Breach, even though it continued for almost five months. As discussed below, the Breach was ultimately uncovered, not through any cybersecurity measure taken by the Company itself, but rather because the Secret Service and an independent security blogger unearthed the story.

96. 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!"

97. 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.



Redacted

98. 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.

99. 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 on its website noting that it was "looking into some unusual activity" and that it would provide "further information as soon as possible."

100. On September 3, 2014, Krebs 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.

101. 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.

102. Unfortunately, because Home Depot had not yet confirmed the Breach, financial institutions were reluctant to cancel and reissue their payment cards. Therefore, the new batches of fraudulently obtained cards continued to have a validity rate of 100 percent.

103. 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. Home Depot still had not confirmed the Breach, so the overwhelming bulk of compromised payment cards had not yet been cancelled. The new batches of fraudulently obtained cards again had a validity rate of nearly 100 percent.



Redacted

104. 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."

105. On September 8, 2014, Home Depot filed an 8-K acknowledging that a security breach had occurred affecting its payment data systems, which could potentially impact customers using payment cards at its U.S. and Canadian stores.

106. In its 8-K, the Company stated that its investigation of the Data Breach began on Tuesday morning, September 2, 2014, immediately after the Company received reports from its banking partners and law enforcement that criminals may have hacked its payment data systems. Home Depot stated that it was offering free identity protection services, including credit monitoring, to any customer who used a payment card at a Home Depot store from April 2014 forward. However, Home Depot failed to warn its customers that their financial information was currently for sale and being used by criminals around the world.

107. 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."

108. 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.

109. Home Depot's failure to institute adequate measures to protect against 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 describing the vulnerabilities on Home Depot's website dated 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.

110. 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…"

111. Krebs on Security reported on September 9, 2014 that "multiple banks say they are seeing evidence that Home Depot stores may be the source of a massive new batch of stolen credit and debit cards that went on sale this morning in the cybercrime underground." Home Depot spokesperson Paula Drank confirmed that "we are looking into some unusual activity and we are working with our banking partners and law enforcement to investigate…. Protecting our customers' information is something we take extremely seriously, and we are aggressively gathering facts at this point while working to protect customers. If we confirm that a breach has occurred, we will make sure customers are notified immediately."

112. On September 18, 2014, Home Depot issued an 8-K confirming that 56 million Home Depot customers' credit cards had been compromised during the period from April to September 2014. Home Depot stated that it had eliminated the malware used in the Data Breach from its U.S. and Canadian networks. The Company further reported that it had completed a "major security project" that would provide enhanced encryption in its U.S. stores and that enhanced encryption would be implemented in its Canadian stores by early 2015. The encryption technology reportedly "locks down payment data through enhanced encryption, which takes raw payment card information and scrambles it to make it unreadable and virtually useless to hackers." Finally, Home Depot decided to "provide credit monitoring services to its customers, increase call center staffing, and pay legal and professional services, all of which are expensed as incurred in a gross amount of approximately $62 million, partially offset by a $27

million receivable for costs the Company believes are reimbursable and probable of recovery under its insurance coverage."

113. According to a *New York Times* report dated September 20, 2014, Home Depot data had already popped up on black markets, and by one estimate, could be used to make up to $3 billion in illegal purchases.

114. In October 2014, Frank Blake, Home Depot's soon-to-be-departing CEO, acknowledged in an interview that: "If we rewind the tape, our security systems could have been better. Data security just wasn't high enough in our mission statement." Blake characterized the Company's data security systems as "desperately out of date."

115. On November 1, 2014, Craig Menear succeeded Frank Blake as Home Depot's Chief Executive Officer.

116. On November 6, 2014, Home Depot filed an 8-K, disclosing additional findings related to the Data Breach. Those findings were:

- Criminals used a third-party vendor's user name and password to enter the perimeter of Home Depot's network. These stolen credentials alone did not provide direct access to the Company's point-of-sale devices.

- The hackers then acquired elevated rights that allowed them to navigate portions of Home Depot's network and to deploy unique, custom-built malware on its self-checkout systems in the U.S. and Canada.

- In addition to the previously disclosed payment card data, separate files containing approximately 53 million email addresses were also taken during the breach. These files did not contain passwords, payment card information or other sensitive personal information. The Company is notifying affected customers in the U.S. and Canada. Customers should be on guard against phishing scams, which are designed to trick customers into providing personal information in response to phony emails.

117. In addition, the 8-K reiterated the news contained in its prior 8-K that it had completed implementation of enhanced encryption of payment data in its U.S. stores. The 8-K continued:

> The new security protection locks down payment card data, taking raw payment card information and scrambling it to make it unreadable and virtually useless to hackers. Home Depot's encryption technology provided by Voltage Security, Inc. has been tested and validated by two independent IT security firms.



Redacted

118. The 8-K stated that implementation of the project was "accelerated" after the Breach was discovered and reiterated that the enhanced encryption would be implemented in Home Depot's Canadian stores by early 2015.

119. Finally, the November 6, 2014 8-K included the following statement regarding "EMV Chip-and-Pin Technology":

> The Company is rolling out EMV chip-and-PIN technology, which adds extra layers of payment card protection for customers. Chip-and-PIN technology was deployed to Canadian stores in 2011. Launched as a project for U.S. stores in January 2013, the project will be completed ahead of the payment industry's deadline.

120. On November 18, 2014, Home Depot issued another 8-K regarding the Data Breach. In its SEC filing, the Company stated as follows:

> We discovered a data breach in the third quarter of fiscal 2014 and are still in the process of determining the full extent of its impact and the impact of related government investigations and civil litigation on our results of operations, which could be material.
>
> Our recent data breach involved the theft of certain payment card information and customer email addresses through unauthorized access to our network. As a result of the breach, we are facing at least 44 civil lawsuits filed in the U.S. and Canada, and other claims may be asserted on behalf of customers, payment card brands, payment card issuing banks, shareholders, or others seeking damages or other related relief, allegedly arising out of the data breach. We are also facing investigations by a number of state and federal agencies. These claims and investigations may adversely affect how we operate our business, divert the attention of management from the operation of the business and result in additional costs and fines. In addition, the governmental agencies investigating the data breach may seek to impose injunctive relief, which could materially increase our data security costs, adversely impact how we operate our systems and collect and use customer information, and put us at a competitive disadvantage with other retailers.

121. Craig Menear succeeded Frank Blake as Chairman of the Board on February 2, 2015.

***Harm to Home Depot***

122. Following the Breach, consumers and financial institutions have filed at least 44 civil actions against Home Depot, claiming that Home Depot failed to take adequate measures to ensure its data systems were protected and to prevent the Data Breach from happening, as well as that Home Depot failed to provide timely notice of the Breach.

123. The consumer plaintiffs allege that, as a result of the Data Breach, they suffered: (a) unauthorized charges on their debit and credit card accounts; (b) theft of their personal and

financial information; (c) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; (d) loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations; (e) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Home Depot data breach; (f) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their payment card and personal information being placed in the hands of criminals and already misused via the sale of consumer plaintiffs' information on the Internet black market; (g) damages to and diminution in value of their personal and financial information entrusted to Home Depot for the sole purpose of purchasing products and services from Home Depot and with the mutual understanding that Home Depot would safeguard consumer data against theft and not allow access to and misuse of their information by others; (h) money paid for products and services purchased at Home Depot stores during the period of the Home Depot data breach in that consumer plaintiffs allegedly would not have shopped at Home Depot had Home Depot disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Home Depot provided timely and accurate notice of the Home Depot data breach; (i) continued risk to their financial and personal information, which remains in the possession of Home Depot and which is subject to further reaches so long as Home Depot fails to undertake appropriate and adequate measures to protect consumer plaintiffs' data in its possession.



Redacted

124. The consumer plaintiffs assert common law claims for negligence, breach of implied contract, and unjust enrichment as well as claims under various consumer protection and data breach notification statutes under the common law of every state and the statutes of nearly every state in the country, and seek damages, injunctive relief, and a declaratory judgment.

125. The financial institution plaintiffs claim that, as a result of the Data Breach, they suffered costs related to canceling and reissuing millions of compromised cards and reimbursing their customers for fraudulent charges. The Financial Institutions assert common law claims for negligence and negligence per se as well as claims for injunctive and declaratory relief and claims under various consumer protection statutes. The financial institution plaintiffs seek damages, injunctive relief, and a declaratory judgment.

126. In addition, several state and federal agencies, including State Attorneys General, have initiated investigations into the events related to the Data Breach, including how it occurred, its consequences, and Home Depot's responses to the Data Breach.

127. In its 10-K filed with the SEC on March 26, 2015, Home Depot reported:

> In the third quarter of fiscal 2014, the Company recorded $43 million of pretax expenses related to the Data Breach, partially offset by a $15 million receivable for costs the Company believes are reimbursable and probable of recovery under its insurance coverage, for pretax net expenses of $28 million. … Expenses include costs to investigate the Data Breach; provide identity protection services, including credit monitoring, to impacted customers; increase call center staffing; and pay legal and other professional services, all of which were expensed as incurred.
>
> …
>
> In addition to the above expenses, the Company believes it is probable that the payment card networks will make claims against the Company. The ultimate amount of these claims will likely include amounts for incremental counterfeit fraud losses and non-ordinary course operating expenses (such as card reissuance costs) that the payment card networks assert they or their issuing banks have incurred. In order for the Company to have liability for such claims, the Company believes it would have to be determined, among other things, that (1) at the time of the Data Breach the portion of the Company's network that handles payment card data was noncompliant with applicable data security standards, and (2) the alleged noncompliance caused at least some portion of the compromise of payment card data that occurred during the Data Breach. Although an independent third-party assessor found the portion of the Company's network that handles payment card data to be compliant with applicable data security standards in the fall of 2013, the process of obtaining such certification for 2014 was ongoing at the time of the Data Breach and the forensic investigator working on behalf of the payment card networks may claim that the Company was not in compliance with those standards at the



Redacted

> time of the Data Breach. As a result, the Company believes it is probable that the payment card networks will make claims against it and that the Company will dispute those claims. .... At this time, the Company believes it is probable that the claims will be asserted and that settlement negotiations will ensue, and believes that a loss in connection with these claims is reasonably possible. ... The Company believes it is reasonably possible that the ultimate amount paid on payment card network claims could be material to the Company's consolidated financial condition, results of operations, or cash flows in future periods.
>
> In addition, at least 44 actions have been filed in courts in the U.S. and Canada, and other claims may be asserted against the Company on behalf of customers, payment card brands, payment card issuing banks, shareholders or others seeking damages or other related relief, allegedly arising from the Data Breach. Furthermore, several state and federal agencies, including State Attorneys General, are investigating events related to the Data Breach, including how it occurred, its consequences and the Company's responses. The Company is cooperating in the governmental investigations, and the Company may be subject to fines or other obligations. While a loss from these matters is reasonably possible, the Company is not able to estimate the costs, or range of costs, related to these matters because the proceedings remain in the early stages, alleged damages have not been specified, there is uncertainty as to the likelihood of a class or classes being certified or the ultimate size of any class if certified, and there are significant factual and legal issues to be resolved. ... The Company believes that it is reasonably possible that the ultimate amount paid on these actions, claims and investigations could be material to the Company's consolidated financial condition, results of operations, or cash flows in future periods.

128. In addition to the costs already incurred and the potential litigation costs, Home Depot's Annual Report disclosed that the Company may incur substantial expenses related to credit card fraud and card reissuance costs for the Company's private label credit card program, as well as incremental expenses and capital investments for remediation activities. According to its 10-K of March 26, 2015, "The Company believes that it is reasonably possible that the ultimate amount paid on these services and claims could be material to the Company's consolidated financial condition, results of operations, or cash flows in future periods."

129. According to the Amended Complaint filed by the financial institutions plaintiffs, "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."



Redacted

## DUTIES OF THE INDIVIDUAL DEFENDANTS

***Fiduciary Duties***

130. By reason of their positions as officers and directors of the Company, each of the Individual Defendants owed and owe Home Depot and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care and were and are required to use their utmost ability to control and manage Home Depot in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of Home Depot and not in furtherance of their personal interest or benefit.

131. Throughout the Relevant Period, to discharge their duties, the officers and directors of Home Depot were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors of Home Depot were required to, among other things: (a) devise and implement a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected; (b) monitor and oversee a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected; (c) ensure that the Company timely and accurately informs customers regarding any breach of their personal and financial information; (d) establish corporate governance and reporting structures effective to inform themselves about data security risks and enable them to oversee data security risk management; (e) conduct the affairs of the Company in an efficient, business-like manner in compliance with all applicable laws, rules, and regulations so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock; and (f) remain informed as to how Home Depot conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices.

132. In addition, the Audit Committee members, pursuant to the Audit Committee Charter, bear the primary responsibility for overseeing risk assessment and management at Home

Depot during the Relevant Period, including the Company's major financial exposures and compliance risks and the steps management takes (or does not take) to monitor and control those exposures and risks. Accordingly, throughout the Relevant Period, the Audit Committee Members had primary responsibility for overseeing risks related to information technology and data privacy and security at Home Depot.

***Breaches of Duties***

133. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as officers and directors of Home Depot, the absence of good faith on their part, and a conscious or reckless disregard for their duties to the Company.

134. For example, the Individual Defendants failed to ensure, among other things, that the Company implemented reasonable measures to protect its customers' personal and financial information, including by maintaining its computer systems in accordance with PCI DSS as required by its contracts with payment card processors and networks. [redacted]

135. The Individual Defendants, because of their positions of control and authority as officers and/or directors of Home Depot, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein. The Individual Defendants also failed to prevent the other Individual Defendants from taking such illegal actions. As a result, and in addition to the damage the Company has already incurred, Home Depot has expended, and will continue to expend, significant sums of money.

136. The Individual Defendants' failure to ensure that the Company took reasonable measures to protect its customers' personal and financial information, as required by its contracts



Redacted

with payment card processors, has caused Home Depot to incur substantial costs, and it will be forced to incur substantial additional costs in the future, in connection with the following, among other things: (i) various investigations into the Breach, including, but not limited to, expenses for legal, investigative, and consulting fees, and liability for potential resulting fines and penalties (ii) defending and paying any settlement or judgment in the class actions brought by financial institutions alleging that they sustained billions of dollars of damages due to the Breach associated with the costs of notifying their customers regarding replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for improper charges; (iii) defending and paying any settlement or judgment in the class actions brought by Home Depot's customers; (iv) defending and paying any settlement or judgment in any litigation brought by the payment card processors; and (v) paying compensation and benefits to the Individual Defendants who have breached their duties to the Company.

137. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs complained of herein. In taking such actions to substantially assist the commission of the wrongdoing complained of herein, each Individual Defendant acted with knowledge of the primary wrongdoing, substantially assisted in the accomplishment of that wrongdoing, or is presumed to have acquiesced to the wrongdoing and was aware of his or her overall contribution to and furtherance of the wrongdoing.

## DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS

138. Plaintiff brings this action derivatively on behalf of Home Depot to redress injuries suffered, and to be suffered, by Home Depot as a direct result of breaches of fiduciary duty and waste of corporate assets, as well as the aiding and abetting thereof, by the Individual Defendants. Home Depot is named as a nominal defendant solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

139. Plaintiff will adequately and fairly represent the interests of Home Depot in enforcing and prosecuting its rights and has hired experienced counsel.

140. Plaintiff was a shareholder of Home Depot at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Home Depot shareholder.

141. Home Depot is controlled by its Board, which at the time this action was commenced, consisted of ten members, nine of whom are named herein. Demand is excused as to the nine Director Defendants for the reasons alleged below.

142. At the time this action was commenced, Home Depot's Board consisted of ten (10) members, nine (9) of whom are named as defendants herein: Bousbib, Brenneman, Brown, Albert Carey, Codina, Foulkes, Katen, Menear, and Vadon (the "Director Defendants"). Plaintiff did not make any demand on the Board to institute this action because such a demand would be futile for all of the reasons set forth below.

143. All of the Director Defendants are disqualified from fairly evaluating the derivative claims because they are responsible for damages suffered by Home Depot as a result of the Company's massive Data Breach.

[redacted]



Redacted

[redacted]

148. Home Depot had the capability of making all of these improvements immediately.

149. Home Depot already possessed the NTP firewall feature of its Symantec software and needed only to activate it, rather than relying upon an antiquated Windows-based system as its firewall. Nonetheless, the Board failed to ensure that the Company install a reasonable firewall to protect its system against intrusion.

150. Home Depot also could have readily updated its antivirus and antispyware software. In fact, the Company had been warned since 2011 that its antivirus and antispyware software was out of date and needed to be replaced, but it failed to do so even while the Data Breach was ongoing.

151. Home Depot also could have encrypted its customer data prior to the Data Breach. Beginning in at least 2009, external consultants warned Home Depot that its failure to encrypt customer data at the point of sale posed a substantial risk, and these warnings were echoed by Home Depot's own employees for years. Home Depot finally purchased the technology to encrypt its customer data in January 2014, [redacted] As a result, only 25% of customer data was encrypted when the Data Breach was discovered. That the encryption could have been implemented well before the Breach occurred is made obvious by the fact that, once the Data Breach was discovered, the Company managed to encrypt the remaining 75% of its customers' data in only eleven (11) days.



Redacted

152. The Board's failure to ensure that the Company abided by the PCI DSS standards in 2014, as required by its contracts with payment card industry members such as Visa and MasterCard, has exposed the Company to massive liability in the form of class actions brought by consumers and financial institutions and the prospect of additional litigation brought by the payment card industry itself. In addition, the Board's failure to ensure that the Company abided by the PCI DSS standards at the time of the breach may have exposed the Company to government investigations and the prospect of substantial fines.

153. The Board's failure of oversight reflects a conscious and deliberate disregard for their fiduciary duties—namely, inaction in the face of circumstances that plainly called for immediate action. As such, the Board faces a substantial likelihood of liability, rendering demand upon them futile.

154. [redacted] Because of their failures to act in the face of a known duty to act to protect the Company, the Director Defendants face a substantial likelihood of liability, and demand against them would be futile.

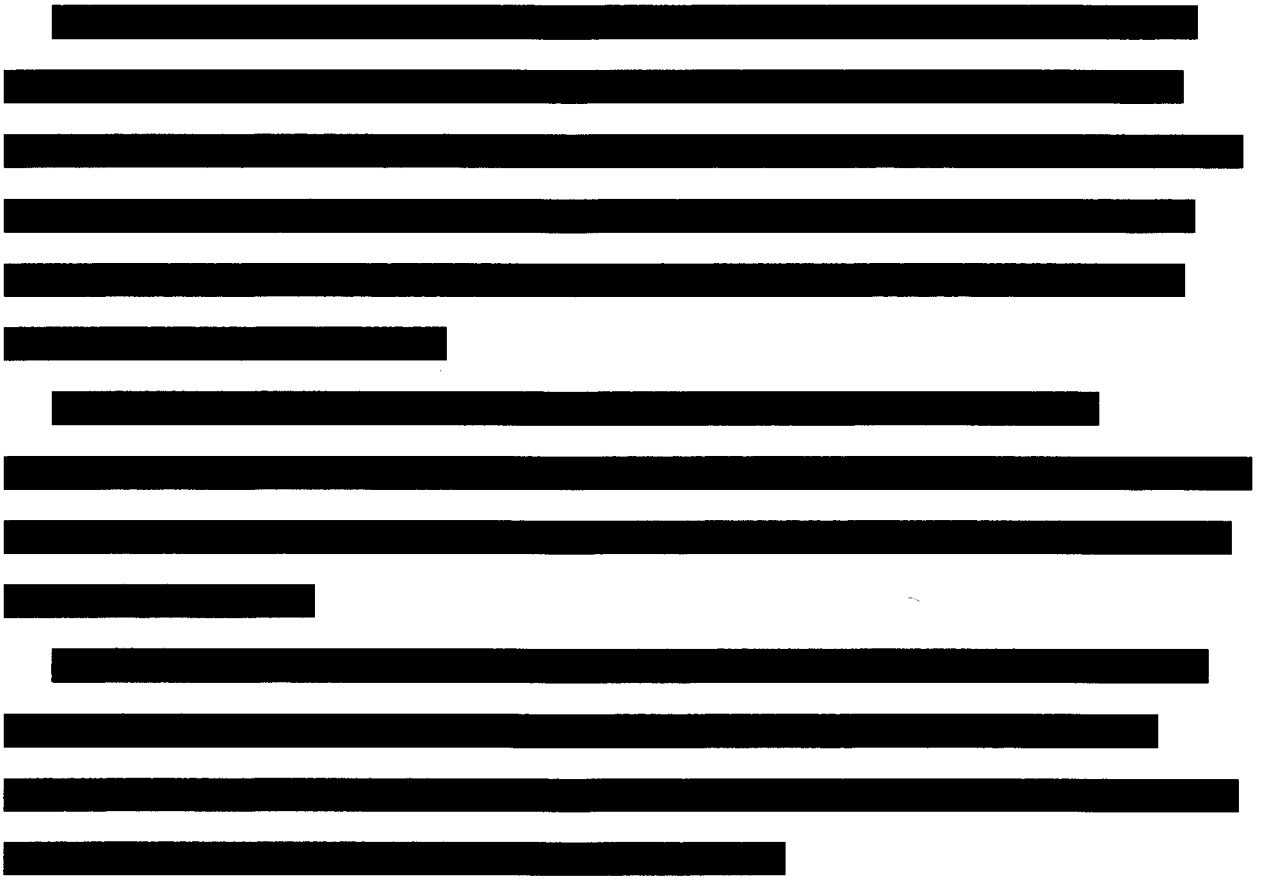
155. Home Depot has been and will continue to be exposed to significant losses due to the wrongdoing complained of herein, yet the Director Defendants have not filed any lawsuits against themselves or others who were responsible for that wrongful conduct to attempt to recover for Home Depot any part of the damages Home Depot suffered and will suffer thereby.

156. Demand upon Individual Defendants Bousbib, Brown, Katen, and Vadon would also be futile for the additional reason that each served as a member of Home Depot's Audit Committee during the Relevant Period.



Redacted

157. Home Depot's Audit Committee has primary responsibility for overseeing risk assessment and management at Home Depot, including the Company's major financial exposures and compliance risks and the steps management takes to monitor and control those risks. The Audit Committee also has primary responsibility for overseeing risks related to information technology and data privacy and security at Home Depot.



161. Because of their failures to act in the face of a known duty to act to protect the Company, these Audit Committee members face a substantial likelihood of liability, and demand against them would be futile.

Additionally, a demand upon defendant Menear would be futile because he lacks independence. As an executive of the Company, Menear does not satisfy New York Stock Exchange director independence standards. Indeed, Menear derives his principal income from Home Depot, including material salary and cash and equity retention awards.



Redacted

[redacted]

163. Finally, demand on the Board would also be futile and is excused because the Board's decisions not to implement adequate corporate governance and risk management procedures necessary to protect the Company from a data breach served no legitimate business purpose. [redacted]

Moreover, the fact that the Company was able to almost immediately implement these critical security measures within only eleven days of it being alerted to the Data Breach further illustrates how there was no legitimate business purpose for the Board's acquiescence to the delays.

164. Plaintiffs also did not make any demand on the other shareholders of Home Depot to institute this action since such demand would be a futile act for at least the following reasons: (i) Home Depot is a publicly held company with approximately 1.3 billion shares outstanding and hundreds of thousands of shareholders; (ii) making a demand on such a number of shareholders would be impossible for plaintiffs who have no way of finding out the names, addresses, or phone numbers of shareholders; and (iii) making demand on all shareholders would force plaintiffs to incur excessive expenses, assuming all shareholders could be individually identified.

## COUNT I

### Against the Individual Defendants for Breach of Fiduciary Duty

165. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

166. As alleged in detail herein, the Individual Defendants, by reason of their positions as officers and directors of Home Depot and because of their ability to control the business and



Redacted

corporate affairs of Home Depot, owed to Home Depot fiduciary obligations of due care and were and are required to use their utmost ability to control and manage Home Depot in a fair, just, honest, and equitable manner.

167. The Officer Defendants breached their duties of loyalty and care by knowingly and in conscious disregard of their fiduciary duties: (i) failing to oversee and manage the risks posed by Home Depot's data security systems and (ii) failing to oversee the (inadequate) internal controls that failed to protect customers' personal and financial information, which led to the theft of over 53 million customers' personal and financial data.

168. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, Home Depot has sustained significant damages, as alleged herein. As a result of the misconduct alleged herein, these defendants are liable to the Company.

169. Plaintiffs, on behalf of Home Depot, have no adequate remedy at law.

**COUNT II**

**Against the Individual Defendants for Waste of Corporate Assets**

170. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

171. The wrongful conduct alleged includes the Individual Defendants' failure to implement adequate internal controls to detect and prevent the breach of the Company's customers' personal and financial information. Under the Individual Defendants' direction and purview, Home Depot's customers became the victims of the biggest data breach in retail history. The Company has already incurred substantial costs in investigating the data breach and cooperating with various government investigations. In addition, the Company anticipates the loss of material amounts due to settlements with the payment card industry providers, such as Visa and MasterCard, and may also lose material amounts due to judgments or settlements in the consumer and financial industry class actions.

172. Further, the Individual Defendants caused Home Depot to waste its assets by paying improper compensation and bonuses to those of its executive officers and directors that breached their fiduciary duties.

173. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

174. Plaintiff, on behalf of Home Depot, has no adequate remedy at law.

**PRAYER FOR RELIEF**

175. WHEREFORE, Plaintiff, on behalf of Home Depot, demands judgment as follows:

a. Against the Individual Defendants and in favor of the Company for the amount of damages sustained by the Company as a result of the Individual Defendants' breaches of fiduciary duty, waste of corporate assets, and aiding and abetting breaches of fiduciary duties;

b. Directing Home Depot to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its shareholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for shareholder vote, resolutions for amendments to the Company's By-Laws or Articles of Incorporation, and taking such other action as may be necessary to place before shareholders for a vote of the following Corporate Governance Policies:

i. a proposal to strengthen the Company's controls over its customers' personal and financial information;

ii. a proposal to create a Board-level committee specifically tasked with monitoring the Company's data security measures;

iii. a proposal to establish new corporate governance and internal controls to enhance Board oversight of the protection of the Company's IT systems and data;

iv. a proposal to establish new, full-time positions at the Company focused on improved data security and risk management procedures;

v. a proposal to establish new, full-time positions in the Company focused on compliance with the Company's data security and risk management best practices;

vi. a proposal to strengthen the Company's disclosure controls; and

vii. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater shareholder input into the policies and guidelines of the Board.

c. Awarding to Home Depot restitution from the Individual Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants;

d. Awarding Plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees, costs, and expenses; and

e. Granting such other and further equitable relief as this Court may deem just and proper.

**JURY DEMAND**

Plaintiffs demand a trial by jury.



Redacted

DATED: August 25, 2015

KEN HODGES LAW

By: _____
Kenneth B. Hodges III
Georgia Bar No. 359155
2719 Buford Highway NE
Atlanta, Georgia 30324
Telephone: (404) 692-0488
Facsimile: (404) 759-6783
ken@kenhodgeslaw.com

SCHUBERT JONCKHEER & KOLBE LLP
Robert C. Schubert
Willem F. Jonckheer
Miranda P. Kolbe
3 Embarcadero Center, Suite 1650
San Francisco, CA 94111
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
rschubert@schubertlawfirm.com
wjonckheer@schubertlawfirm.com
mkolbe@schubertlawfirm.com

*Attorneys for Plaintiff Mary Lou Bennek*



Redacted