UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

Charles E. Chorman, individually and on behalf of all others similarly situated,

Plaintiff,

v.

Home Depot U.S.A., Inc., a Delaware corporation,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

Plaintiff Charles E. Chorman, by and through his undersigned counsel, bring this Class Action Complaint against Defendant Home Depot U.S.A., Inc., on behalf of himself and all others similarly situated, and allege, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff bring this class action against Defendant Home Depot U.S.A., Inc. ("Home Depot") for its failure to secure and safeguard its customers' credit and debit card numbers and other payment card data ("PCD"), personally identifiable information such as the cardholder's names, mailing addresses, and other personal information ("PII") (collectively, "Private Information"), and for failing to provide timely, accurate and adequate notice to Plaintiff and other Class members that their Private Information had been stolen and precisely what types of information were stolen.

2. Beginning in or around April 2014, hackers utilizing malicious software accessed the point-of-sale systems at Home Depot locations throughout the United States and stole copies of Home Depot customers' Private Information (the "Data Breach"). In early September 2014,

Home Depot customers' Private Information was placed for sale on an underground website notorious for offering PII and PCD.

3. On September 3, 2014, after security blogger Brian Krebs first reported news of the Data Breach, Home Depot admitted that it did not become aware of the Data Breach until September 2, 2014. Six days later, on September 8, 2014, Home Depot confirmed on its website that it had allowed a massive breach of its customers' Private Information to occur in 2014, stating that its "systems have in fact been breached, which could potentially impact any customer that has used their payment card at our U.S. and Canadian stores, from April forward."[1] Home Depot's security protocols were so deficient that the Data Breach continued for nearly five months while Home Depot failed to even detect it – this despite widespread knowledge of the malicious software (or malware) used to perpetrate the Data Breach, which was a variant of the same malware used to perpetrate an earlier, notorious, and widely reported data breach affecting the retailer Target Corporation.[2] On September 15, 2014, Home Depot published a notice in USA Today regarding the breach but claimed that no debit card pin numbers were compromised, a statement which is not accurate.

4. Home Depot has yet to fully disclose what types of Private Information were stolen, but concedes that "[p]ayment card information such as name, credit card number, expiration date, cardholder verification value and service code for purchases made at Home Depot stores in 2014, from April on" were "compromised."[3]

5. Reuters reports that "experts fear the attackers may have gotten away with more

---

[1] <https://corporate.homedepot.com/mediacenter/pages/statement1.aspx> (last visited Sept. 24, 2014).

[2] <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited Sept. 24, 2014).

[3] <https://corporate.homedepot.com/MediaCenter/Documents/Required%20Regulatory%20Notice.PDF> (last visited Sept. 24, 2014).

than 40 million payment cards, which would exceed the number taken in last year's unprecedented data breach on Target Corp."[4] Home Depot concedes that customers who shopped at its stores as far back as April 2014 were exposed. Thus, the Data Breach extended for nearly five months, including the busy summer season — far longer than the three-week Target data breach.

6. Home Depot could have prevented this Data Breach. The malicious software used in the Data Breach was a variant of "BlackPOS," the identical malware strain that hackers used in last year's data breach at Target. While many retailers, banks and card companies responded to recent breaches, including the Target breach, by adopting technology that helps makes transactions more secure, Home Depot did not do so.

7. Home Depot disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Private Information. On information and belief, Plaintiff's and Class members' Private Information was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiff's and Class members' Private Information was compromised and stolen.

PARTIES

8. Plaintiff Charles E. Chorman is an individual and resident of Clay County, Florida. Between April 1, 2014 and September 8, 2014, Plaintiff used a debit card, which

[4] <http://www.reuters.com/article/2014/09/09/home-depot-dataprotection-breach-probe-idUSL1N0RA1DL20140909> (last visited Sept. 24, 2014).

required that he provide Home Depot with his pin number at the time of the transactions, to make purchases of consumer goods at the Home Depot store located in Clay County, Florida. On September 5, 2014, Plaintiff was contacted by the financial institution where he maintained his checking account which was linked to his debit card, and he was informed that two unauthorized withdrawals in the amount of $560 each had been made from his account and one unauthorized purchase in the amount of $504.90 had been made using his debit card information. These transaction which he did not make or authorize, were made even though he had possession of his debit card and his pin at the time these transactions were made. To date, Plaintiff has not received any direct notice from Home Depot about the Data Breach. Plaintiff has reported the theft of his debit card information to the Clay County Sheriff's Department. The detective who interviewed Plaintiff regarding the theft of his Private Information informed him that a total of 90 account holders of the financial institution where Plaintiff maintained his account had their accounts comprised from the breach that is the subject of this complaint.

9. Home Depot is a Delaware corporation headquartered in Atlanta, Georgia. Home Depot operates retail stores throughout the United States, including throughout Florida and including the Florida location where Plaintiff's purchases were made.

JURISDICTION AND VENUE

10. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000, exclusive of interest and costs, and this is a class action in which more than two-thirds of the proposed plaintiff class, on the one hand, and defendant Home Depot, on the other, are citizens of different states.

11. This Court has jurisdiction over Home Depot because it is authorized to conduct

business in Florida, it maintains substantial contacts in the state as it owns numerous retail stores in the state which sells consumer goods to consumers, such as those purchased by Plaintiff, and it advertises in a variety of media throughout Florida. Through its business operations in Florida or otherwise, Home Depot intentionally avails itself of the markets within Florida to render the exercise of jurisdiction by this Court just and proper.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District as Home Depot operates retail locations within this District, Plaintiff resides here, and his purchases took place at Home Depot's retail store located within this District.

FACTUAL BACKGROUND

A. Home Depot and its Private Information Collection Practices

13. Home Depot operates approximately 1,977 home improvement and construction retail stores in the United States. Home Depot is the fifth largest retailer in the United States, behind Walmart, Kroger, Costco, and Target, with annual U.S. sales in 2013 of $69,951 billion.

14. When consumers make consumer purchases at Home Depot retail stores using credit or debit cards, Home Depot collects PCD related to that card including the card holder name, the account number, expiration date, card verification value (CVV), and PIN data for debit cards. Home Depot stores the PCD in its point-of-sale system and transmits this information to a third party for completion of the payment. Home Depot also collects and stores PII, including but not limited to customer names, mailing addresses, phone numbers, and email addresses.

15. Through its Privacy Policy, which is available on its website, Home Depot advises consumers about the categories of Private Information it collects:

Information We Collect

Contact information

We may collect the names and user names of our customers and other visitors. Additionally, we may collect your purchase history, billing and shipping addresses, phone numbers, email addresses, and other digital contact information. We may also collect information that you provide us about others.

Payment information

When you make a purchase we collect your payment information, including information from your credit or debit card, check, PayPal account or gift card. If you apply for a The Home Depot credit card or a home improvement loan, we might collect information related to your application.

Returns information

When you return a product to our stores or request a refund or exchange, we may collect information from you and ask you to provide your government issued ID. We use the information we collect from you and capture off of your government issued ID to help prevent fraud. To learn more about our Returns Policy, click here.

Demographic information

We may collect information about products or services you like, reviews you submit, or where you shop. We might also collect information like your age or gender.

Location information

If you use our mobile websites or applications, we may collect location data obtained from your mobile device's GPS. If you use our websites, we may collect location data obtained from your IP address. We use this location data to find our nearest store to you, product availability at our stores near you and driving directions to our stores.

Other information

If you use our websites, we may collect information about the browser you are using. We might track the pages you visit, look at what website you came from, or what website you visit when you leave us. We collect this information using the tracking tools described here. To control those tools, please read the Your

Privacy Preferences section.[5]

16. Home Depot stores massive amounts of PII and PCD on its servers and utilizes this information to maximize its profits through predictive marketing and other marketing techniques.

B. Consumers Rely On Home Depot's Private Information Security Practices

17. Consumers place value in data privacy and security, and they consider it when making purchasing decisions. Plaintiff would not have made purchases at Home Depot, or would not have paid as much for them, had he known that Home Depot does not take all necessary precautions to secure their personal and financial data. Home Depot failed to disclose its negligent and insufficient data security practices and consumers relied on this omission to make purchases at Home Depot.

18. Furthermore, when consumers purchase goods at a national retailer, such as Home Depot, they assume that its data security practices and policies are state-of-the-art and that the retailer will use part of the purchase price that consumers pay for such state-of-the-art practices. Consumers thus enter into an implied contract with Home Depot that Home Depot will adequately secure and protect their Private Information, and will use part of the purchase price of the goods to pay for adequate data security measures. In fact, rather than use those moneys to implement adequate data security policies and procedures, Home Depot failed to provide reasonable security measures, thereby breaching its implied contract with Plaintiffs.

C. Stolen Private Information Is Valuable to Hackers and Thieves

19. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. PII data is often easily taken because it may be less

[5] <http://www.homedepot.com/c/Privacy_Security> (hyperlinks omitted) (last visited Sept. 24, 2014).

protected and regulated than payment card data.

20. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they wouldn't pay for it or aggressively seek it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."[6] Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

21. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id.* PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of thefts and unauthorized access have been the subject of many media reports. One form of identity theft has been branded as "synthetic identity theft." It occurs when thieves create new identities by combining real and fake identifying information then using those identities to open new accounts. "This is where they'll take your Social Security number, my name and address, someone else's birthday and they will combine them into the equivalent of a bionic person," said Adam Levin, chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft, experts said. "It's tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person," Levin has said. In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number.

22. Unfortunately, and as will be alleged below, despite all of this publicly available

[6] Verizon 2014 PCI Compliance Report, available at <http://www.nocash.info.ro/wp-content/uploads/2014/02/ Verizon_pci-report-2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited Sept. 24, 2014).

knowledge of the continued compromises of PII in the hands of other third parties, such as retailers, Home Depot's approach at maintaining the privacy of Plaintiff's and Class members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

D. Home Depot Failed to Segregate PCD From PII

23. Unlike PII data, PCD (or payment card data) is heavily regulated. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

24. "PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data."[7]

25. One PCI requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code.

26. "Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement."[8] However, segregation is recommended because among other reasons, "[i]t's not just cardholder data that's important; criminals are also after personally identifiable information (PII) and corporate data."[9]

27. Illicitly obtained PII and PCI, sometimes aggregated from different data breaches, is sold on the black market, including on websites, as a product at a set price.[10]

E. The 2014 Data Breach at Home Depot

28. On September 2, 2014, Home Depot's banking partners and law enforcement

---

[7] PCI DSS v. 2 at 5 (2010) (hereafter PCI Version 2).

[8] *Id.* at 10.

[9] *See* Verizon Report at 54.

[10] *See, e.g.*, <http://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth> (last visited Sept. 24, 2014).

officials notified the retailer of a potential data breach involving the theft of its customers' credit card and debit card data.

29. That same day, multiple banks began reporting evidence that Home Depot stores were the likely source of a massive batch of stolen card data that went on sale that morning at rescator.cc, the same underground cybercrime shop that sold millions of cards stolen in the 2013 attack on Target. [11]

30. Specifically, according to security blogger Brian Krebs of Krebs on Security (the "Krebs Report"), the cybercrime store rescator.cc (the "Rescator website") listed consumer credit cards for sale that, with the unique ZIP code and other card data, at least four banks had traced back to previous transactions at Home Depot.

31. The Krebs Report explained that "experienced crooks prefer to purchase cards that were stolen from stores near them, because they know that using the cards for fraudulent purchases in the same geographic area as the legitimate cardholder is less likely to trigger alerts about suspicious transactions — alerts that could render the stolen card data worthless for the thieves."[12] The Krebs Report indicated a "staggering 99.4 percent overlap" between the unique ZIP codes represented on the Rescator website and those of Home Depot stores, strongly suggesting that the source of the breached credit card data was from Home Depot.

32. The ZIP code information the Krebs Report pulled from the Rescator website appears to represent the vast majority, if not all, of Home Depot's approximately 2,000 domestic retail locations. The Krebs Report further indicated that, based on conversations with affected banks, this data breach "probably started in late April or early May" and may be ongoing,

---

[11] <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited Sept. 24, 2014).

[12] <http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/> (last visited Sept. 24, 2013).

potentially dwarfing the 40 million debit and credit cards affected by the recent Target data breach (which had 1,800 stores affected during a period of approximately 3 weeks).

33. On September 3, 2014, Home Depot could not confirm whether a data breach occurred, but indicated it first learned of a "potential breach" on September 2, 2014, at least one day before the Krebs Report.[13]

34. Indeed, after this news broke, Home Depot released an ambiguous and uninformative statement buried on its corporate site – and not the Internet site visited by consumers – concerning the Data Breach that failed to confirm the breach, and still did not notify affected customers directly:

> **Message to our customers about news reports of a possible payment data breach.**
>
> We're looking into some unusual activity that might indicate a possible payment data breach and we're working with our banking partners and law enforcement to investigate. We know that this news may be concerning and we apologize for the worry this can create. If we confirm a breach has occurred, we will make sure our customers are notified immediately.[14]

35. On September 8, 2014, Home Depot confirmed that its systems "have in fact been breached, which could potentially impact any customer that has used their payment card at our U.S. and Canadian stores, from April forward."[15]

36. Home Depot has not indicated whether social security numbers, PIN numbers and dates of birth were compromised, nor has it disclosed whether the wide range of other PII that it collects, including names, addresses, telephone numbers, mobile telephone numbers, driver's

---

[13] <http://online.wsj.com/articles/home-depot-tries-to-reassure-customers-about-possible-data-breach-1409743851> (last visited Sept. 24, 2014).

[14] <https://corporate.homedepot.com/mediacenter/pages/statement1.aspx> (last visited Sept. 24, 2014).

[15] <https://corporate.homedepot.com/mediacenter/pages/ statement1.aspx> (last visited Sept. 24, 2014).

license numbers, bank account numbers, email addresses, computer IP addresses, and location information, were disclosed in the breach.[16]

37. Without such detailed disclosure, Plaintiff and Class members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

38. If fraud were occurring from late April to early September of 2014, because hackers already had their hands on cardholder data and PII, credit card company analytics and other methods (undercover investigations of the black market) would likely have discovered it before September 2, 2014. Home Depot has failed to provide a cogent picture of how the Data Breach occurred and its full effects on consumers' PII and PCD information.

39. Hacking is often accomplished in a series of phases to include reconnaissance, scanning for vulnerabilities and enumeration of the network, gaining access, escalation of user, computer and network privileges, maintaining access, covering tracks and placing backdoors. On information and belief, while hackers scoured Home Depot's networks to find a way to access PCD, they had access to and collected the PII stored on Home Depot's networks.

40. "The stolen card data being offered for sale on rescator.cc includes both the information needed to fabricate counterfeit cards *as well as the legitimate cardholder's full name* and the city, state and ZIP of the Home Depot store from which the card was stolen."[17] Information pertaining to the cardholder's location allows hackers to obtain a cardholder's Social Security number and date of birth, further increasing the risk of identity theft (above and beyond fraudulent credit and/or debit card transactions) for affected Home Depot customers.

---

[16] <http://www.homedepot.com/c/Privacy_Security> (last visited Sept. 24, 2014).

[17] <http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/> (last visited Sept. 24, 2014).

41. Thieves already are using the Private Information stolen from Home Depot to commit actual fraud. Some thieves are using the Private Information to change a cardholder's PIN numbers on stolen debit cards and to make ATM withdrawals from Home Depot customer's accounts. On September 8, 2014, a bank located on the West Coast reported that it "lost more than $300,000 in two hours today to PIN fraud on *multiple debit cards that had all been used recently at Home Depot.*"[18] (emphasis added). On that same day, the Krebs Report advised that multiple financial institutions had reported "a steep increase over the past few days in fraudulent ATM withdrawals on customer accounts."

42. The Data Breach was caused and enabled by Home Depot's knowing violation of its obligations to abide by best practices and industry standards in protecting its customers' Private Information.

43. In this regard, the software used in the attack was a variant of "BlackPOS," a malware strain designed to siphon data from cards when they are swiped at infected point-of-sale systems.[19] Hackers had previously utilized BlackPOS in other recent cyber-attacks, including last year's breach at Target. While many retailers, banks and card companies have responded to these recent breaches by adopting technology and security practices that help makes transactions and stored data more secure, Home Depot did not do so. In light of the breach, however, Home Depot now has announced that it plans to have chip-enabled checkout terminals at all of its U.S. stores by the end of 2014.[20]

---

[18] *Id.*

[19] http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/ (last visited September 12, 2014).

[20] <http://money.msn.com/businessnews/article.aspx?feed=AP&date=20140909&id=17914998&ocid=ansmony11> (last visited September 12, 2014).

F. This Data Breach Will Result In Identity Theft and Identify Fraud

44. Home Depot failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the data breach.

45. The ramifications of Home Depot's failure to keep Plaintiff's and Class members' data secure are severe.

46. The information Home Depot compromised, including Plaintiff's identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC").[21] Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

47. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[22]

48. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud."[23] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

---

[21] FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at* <http://www.dcsheriff.net/community/documents/id-theft-tool-kit.pdf> (last visited Sept. 24, 2014).

[22] FTC, Signs of Identity Theft, available at <http://www.consumer.ftc.gov/articles/ 0271-signs-identity-theft> (last visited Sept. 24, 2014).

[23] See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at <www.javelinstrategy.com/brochure/ 276> (last visited Sept. 24, 2014) (the "2013 Identity Fraud Report").

49. Identity thieves can use personal information such as that of Plaintiff and Class members, which Home Depot failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years. The IRS paid out 43.6 billion in potentially fraudulent returns in 2012, and the IRS identified more than 2.9 million incidents if identity theft in 2013. The IRS has described identity theft as the number one tax scam for 2014.

50. Among other forms of fraud, identity thieves may get medical services using consumers' compromised personal information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

51. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[24] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id.* at 11.

52. Annual monetary losses from identity theft are in the billions of dollars.

53. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[25]

---

[24] Victims of Identity Theft, 2012 (Dec. 2013) at 10, available at <http://www.bjs.gov/content/pub/pdf/vit12. pdf> (last visited Sept. 24, 2014).

[25] *See* 2013 Identity Fraud Report.

54. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

55. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

G. Plaintiff and Class Members Suffered Damages

56. The Data Breach was a direct and proximate result of Home Depot's failure to properly safeguard and protect Plaintiff's and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Home Depot's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Private Information to protect against reasonably foreseeable threats to the security or integrity of such information.

57. Plaintiff's and Class members' Private Information is private and sensitive in nature and was left inadequately protected by Home Depot. Home Depot did not obtain

[26] GAO, Report to Congressional Requesters, at p.33 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (emphases added) (last visited Sept. 24, 2014).

Plaintiff's and Class members' consent to disclose their Private Information to any other person as required by applicable law and industry standards.

58. As a direct and proximate result of Home Depot's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

59. Home Depot's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit/debit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet card black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of

their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

h. overpayments to Home Depot for products purchased during the Data Breach in that a portion of the price paid for such products by Plaintiffs and Class members to Home Depot was for the costs of reasonable and adequate safeguards and security measures that would protect customers' Private Information, which Home Depot did not implement and, as a result, Plaintiffs and Class members did not receive what they paid for and were overcharged by Home Depot;

i. the 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; and

j. deprivation of rights they possess under the the Florida Deceptive and Unfair Trade Practices Act (FDUTPA);

k. **Plaintiff's economic injury is also described in Paragraph 8.**

60. Plaintiff also purchased products he otherwise would not have purchased, or paid more for those products and services than they otherwise would have paid.

61. Notwithstanding Home Depot's wrongful actions and inaction and the resulting Data Breach, Home Depot has offered consumers only one year of credit monitoring and identity theft protection services. This offer is insufficient because, *inter alia*, it does not address many

categories of damages being sought. The cost of adequate and appropriate coverage, or insurance, against the loss position Home Depot has placed Plaintiff and Class members in, is ascertainable and is a determination appropriate for the trier of fact.

62. Home Depot's offer of one-year of free identity protection services, including credit monitoring, is also insufficient because, as the GAO reported, the PII/PCD could be held by criminals and used to commit fraud after the one year of credit monitoring and identity theft protection expires. While the Private Information of Plaintiff and members of the Class has been stolen, the same or a copy of the Private Information continues to be help by Home Depot. Plaintiff and members of the Class have an undeniable interest in insuring that this information is secure and not subject to further theft.

CLASS ACTION ALLEGATIONS

63. Plaintiff seeks relief in his individual capacity and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks certification of a Nationwide class and a Florida class. The national class is initially defined as follows:

> All persons residing in the United States whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014 (the "Nationwide Class").

64. The Florida Class is initially defined as follows:

> All persons residing in Florida whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014 (the "Florida Class).

65. Excluded from each of the above Classes are Home Depot, including any entity in which Home Depot has a controlling interest, is a parent or subsidiary, or which is controlled by Home Depot, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Home Depot. Also excluded are the judges and court

personnel in this case and any members of their immediate families.

66. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, Home Depot has acknowledged that 56 million debit and credit cards were affected by the breach.

67. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Home Depot violated the Florida Deceptive and Unfair Trade Practices Act (FDUTPA) by failing to implement reasonable security procedures and practices;

b. Whether Home Depot violated FDUTPA by failing to promptly notify class members their personal information had been compromised;

c. Whether class members may obtain an injunctive relief against Home Depot under FDUTPA to require that it safeguard, or destroy rather than retain the Private Information of Plaintiff and Class members ;

d. What security procedures and data-breach notification procedure should Home Depot be required to implement as part of any injunctive relief ordered by the Court;

e. Whether Home Depot has an implied contractual obligation to use reasonable security measures;

f. Whether Home Depot has complied with any implied contractual obligation to use reasonable security measures;

g. What security measures, if any, must be implemented by Home Depot to comply with its implied contractual obligations;

h. Whether Home Depot violated FDUTPA in connection with the actions described herein; and

i. The nature of the relief, including equitable relief, to which Plaintiff and the Class members are entitled.

68. All members of the purposed Classes are readily ascertainable. Home Depot has access to addresses and other contact information for millions of members of the Classes, which can be used for providing notice to many Class members.

69. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class members because Plaintiff's information, like that of every other class member, was misused and/or disclosed by Home Depot.

70. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

71. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

72. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Home Depot's violations of law

inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

73. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Home Depot has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

74. Plaintiff incorporates the substantive allegations contained in Paragraphs 1 through 73 as if fully set forth herein.

75. Home Depot solicited and invited Plaintiff and Class members to purchase products at Home Depot's stores using their credit or debit cards. Plaintiff and Class members accepted Home Depot's offers and used their credit or debit cards to purchase products at Home Depot's stores during the period of the Data Breach.

76. When Plaintiff and Class members provided their PII and PCD to Home Depot to make purchases at Home Depot's stores, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards, Plaintiff and Class members entered into implied contracts with Home Depot pursuant to which Home Depot agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members if their data had been breached and compromised.

77. Each purchase at a Home Depot store made by Plaintiff and Class members using their credit or debit card was made pursuant to the mutually agreed-upon implied contract with Home Depot under which Home Depot agreed to safeguard and protect Plaintiff's and Class

members' PII and PCD, including all information contained in the magnetic stripe of Plaintiff's and Class members' credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

78. Plaintiff and Class members would not have provided and entrusted their PII and PCD, including all information contained in the magnetic stripes of their credit and debit cards, to Home Depot to purchase products at Home Depot's stores in the absence of the implied contract between them and Home Depot.

79. Plaintiff and Class members fully performed their obligations under the implied contracts with Home Depot.

80. Home Depot breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the PII and PCD of Plaintiff and Class members and by failing to provide timely and accurate notice to them that their PII and PCD was compromised in and as a result of the Data Breach.

81. As a direct and proximate result of Home Depot's breaches of the implied contracts between Home Depot and Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail in Paragraphs 8 and 56 through 62 of this Class Action Complaint.

COUNT II
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

82. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 73 as if fully set forth in this Count.

83. Upon accepting and storing Plaintiff's and Class Members' PII in their respective computer database systems, Defendant undertook and owed a duty to Plaintiff and Class

Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Defendant knew, acknowledged and agreed that the PII was private and confidential and would be protected as private and confidential.

84. The law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiff and the Class so that Plaintiff and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

85. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiff and Class Members and then by failing to provide Plaintiff and Class Members any information regarding the breach until February of 2014. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

86. Defendant also breached its duty to Plaintiff and the Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the PII with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiff's and Class Members' PII, misuse the PII and intentionally disclose it to others without consent.

87. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen and misused,

Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' PII during the time it was within Defendant's possession or control.

88. Further, through its failure to provide timely and clear notification of the data breach to consumers, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

89. Upon information and belief, Defendant improperly and inadequately safeguarded PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access.

90. Defendant's failure to take proper security measures to protect Plaintiff's and Class Members' sensitive PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' PII.

91. Defendant failed to take proper security measures to protect Plaintiff's and Class Members' sensitive PII. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' PII; and failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive PII had been compromised.

92. Neither Plaintiff nor the other Class Members contributed to the data breach and subsequent misuse of their PII as described in this Complaint.

93. As a direct and proximate cause of Defendant's conduct, Plaintiff and the Class

suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members and/or filing false tax returns; and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
Violations of Florida's Unfair and Deceptive Trade Practices Act (On behalf of Plaintiff and the Florida Class)

94. Plaintiff repeats and incorporates the allegations contained in paragraphs 1 through 73 as if fully set forth in this Count.

95. The Florida Unfair and Deceptive Trade Practices Act (hereinafter "FUDTPA") is expressly intended to protect "consumers" like Plaintiff and Class Members from unfair or deceptive trade practices.

96. Plaintiff and Class Members have a vested interest in the privacy, security and integrity of their PII, therefore, this interest is a "thing of value" as contemplated by FUDTPA.

97. Defendant is a "person" within the meaning of the FUDTPA and, at all pertinent times, was subject to the requirements and proscriptions of the FUDTPA with respect to all of their business and trade practices described herein.

98. Plaintiff and Class Members are "consumers" "likely to be damaged" by Defendant's ongoing deceptive trade practices.

99. Defendant's unlawful conduct as described in this Complaint, was facilitated,

directed, and emanated from Defendant's headquarters to the detriment of Plaintiff and Class Members.

100. Defendant engaged in unfair and deceptive trade practices by holding itself out as providing as secure online environment and by actively promoting trust online with consumers, which created in consumers' minds a reasonable expectation of privacy to all consumers by promising that consumers' PII is safe with Defendant, but then failed to take commercially reasonable steps to protect the PII with which it is entrusted.

101. Defendant violated FUDTPA by failing to properly implement adequate, commercially reasonable security measures to protect consumers' sensitive PII.

102. Defendant also violated FUDTPA by failing to immediately notify affected Plaintiff and Class Members of the nature and extent of the data breach.

103. Home Depot's acts, omissions and conduct also violate the unfair component of FUDTPA because Home Depot's acts, omissions and conduct, as alleged herein, offended public policy and constitutes immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other Class members. The gravity of Home Depot's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Home Depot's legitimate business interests, other than Home Depot's conduct described herein.

104. Defendant failed to properly implement adequate, commercially reasonable security measures to hold this information in strict confidence, failed to safeguard Plaintiff's and Class members' PII, and failed to protect against the foreseeable loss and misuse of this information.

105. Plaintiff and Class members have suffered ascertainable losses as a direct result of

Defendant's employment of unconscionable acts or practices, and unfair or deceptive acts or practices.

106. By failing to disclose that it does not enlist industry standard security practices, which render Home Depot's products and services particularly vulnerable to data breaches, Home Depot engaged in a fraudulent business practice that is likely to deceive a reasonable consumer.

107. A reasonable consumer would not have purchased a product at a Home Depot store with a credit or debit card had she known the truth about Home Depot's security procedures. By withholding material information about Home Depot's security practices, Home Depot was able to convince customers to provide and entrust their Private Information to Home Depot. Had Plaintiff known truth about Home Depot's security procedures, he would not have made purchases at Home Depot, or would not have paid as much for them.

108. Home Depot's failure to disclose that it does not enlist industry standard security practices also constitutes an unfair business practice under the FDUTPA. Home Depot's conduct is unethical, unscrupulous, and substantially injurious to the Florida Class. Whereas Home Depot's competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Home Depot has not—to the detriment of its customers and to competition.

109. As a result of Home Depot's violations of the FDUTPA, Plaintiff and the other members of the Contract Class are entitled to injunctive relief including, but not limited to: (1) ordering that Home Depot utilize strong industry standard encryption algorithms for encryption keys that provide access to stored customer data; (2) ordering that Home Depot implement the use of its encryption keys in accordance with industry standards; (3) ordering that Home Depot,

consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on Home Depot's systems on a periodic basis; (4) ordering that Home Depot engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Home Depot audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that Home Depot, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Home Depot is compromised, hackers cannot gain access to other portions of Home Depot's systems; (7) ordering that Home Depot purge, delete, destroy in a reasonable secure manner customer data not necessary for its provisions of services; (8); ordering that Home Depot, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Home Depot, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to consumers who purchase Home Depot products and services through the internet; (10) ordering that Home Depot, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (11) ordering Home Depot to meaningfully educate its customers about the threats they face as a result of the loss of their PII to third parties and the theft of Home Depot's source code, as well as the steps Home Depot's customers must take to protect themselves.

110. As a result of Home Depot's violations of the FDUTPA, Plaintiff and Class members have suffered injury in fact and lost money or property, as detailed in Paragraphs 8 and

56 through 62 of this Class Action Complaint. Plaintiff purchased products or services he otherwise would not have purchased, or paid more for those products and services than he otherwise would have paid. Plaintiff requests that the Court issue sufficient equitable relief to restore Class members to the position they would have been in had Home Depot not engaged in unfair competition, including by ordering restitution of all funds that Home Depot may have acquired as a result of its unfair competition.

111. Under FDUPTA, Plaintiff and the Class are entitled to preliminary and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiff and the Class seek equitable relief and to enjoin Defendant on terms that the Court considers appropriate.

112. Defendant's conduct caused and continues to cause substantial injury to Plaintiff and Class Members. Unless preliminary and permanent injunctive relief is granted, Plaintiff and the Class will suffer harm, Plaintiff and the Class Members do not have an adequate remedy at law, and the balance of the equities weighs in favor of Plaintiff and the Class.

113. At all material times, Defendant's deceptive trade practices are willful within the meaning of FUDTPA and, accordingly, Plaintiff and the Class are entitled to an award of attorneys' fees, costs and other recoverable expenses of litigation.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Home Depot, as follows:

A. For an Order certifying the Nationwide Class and Florida Class as defined herein, and appointing Plaintiff and their Counsel to represent the Nationwide Class and Florida Class;

B. For equitable relief enjoining Home Depot from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class members' private information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members;

C. For equitable relief compelling Home Depot to utilize appropriate methods and policies with respect to consumer data collection, storage and safety and to disclose with specificity to Class members the type of PII and PCD compromised.

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Home Depot's wrongful conduct;

E. For an award of actual damages, compensatory damages, in an amount to be determined;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

G. Such other and further relief as this court may deem just and proper.

Dated: September 26, 2014

Respectfully submitted,

/s/

JOHN A. YANCHUNIS
Florida Bar No. 324681
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com

Tina Wolfson
Robert Ahdoot
Theodore W. Maya

Bradley King
Keith Custis (Of Counsel)
AHDOOT & WOLFSON, PC
10850 Wilshire Blvd., Suite 370
Los Angeles, California 90024
Telephone: 310-474-9111
Facsimile: 310-474-8585

PAUL C. WHALEN
LAW OFFICES OF PAUL C. WHALEN, P.C.
768 Plandome Road
Manhasset, New York 11030
Telephone: (516) 627-5610
Facsimile: (212) 658-9685

Counsel for Plaintiff