IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA

JOHN J. HICKEY, KELLY TOMS, SUNTZU ENTERPRISES, INC., and CONSTRUCTIVE BUILDING SOLUTIONS, LLC, individually and on behalf of all others similarly situated, Plaintiffs, v. THE HOME DEPOT, INC., a Delaware corporation, and HOME DEPOT U.S.A., Inc. Defendant.	)	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs John J. Hickey, Kelly Toms, Suntzu Enterprises, Inc., and Constructive Building Solutions, LLC bring this Class Action Complaint against Defendants The Home Depot, Inc. and Home Depot U.S.A., Inc. (hereinafter collectively, "Defendant," "Home Depot" or the "Company"), individually and on behalf of all others similarly situated, and complain and allege upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

INTRODUCTION AND SUMMARY OF ACTION

1. Plaintiffs bring this class action against Home Depot for its failure to secure and safeguard its customers' personal financial data, personal identifying information and private information ("Private Information" or "PII").

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 Canada and absconded with customers' debit and credit card information, as well as the city, state, and ZIP code of the specific location where the card was used. In early September 2014, this information was placed for sale on an underground website notorious for offering stolen card data.

3. Home Depot admits that it did not become aware of any potential breach for at least *five months*, until September 2, 2014. Six days later, on September 8, 2014, Home Depot confirmed on its website that it had allowed a massive breach (the "Security 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 to September*."[1]

4. Home Depot's security protocols were so deficient that the Security Breach continued for nearly five months while the Company failed to even detect it – this despite widespread knowledge of the malicious software (or malware) used to perpetrate the Security Breach, which was a variant of the same malware used to perpetrate an earlier, notorious, and widely reported data breach affecting the retailer Home Depot Corporation.[2]

5. The inadequacy of Home Depot's security protocols have even been confirmed by former employees of the Company, who believe that "despite alarms as far back as 2008, Home Depot was slow to raise its defenses," even in the face of warnings from its own computer that

[1] https://corporate.homedepot.com/mediacenter/pages/statement1.aspx (last visited December 18, 2014) (emphasis added).

[2] http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/ (last visited December 18, 2014).

the Company was "easy prey for hackers."[3] According to the former employees, Home Depot "relied on outdated software to protect its network and scanned systems that handled customer information irregularly."[4] These concerns were dismissed by Home Depot management.[5]

6. On September 15, 2014, Home Depot published a notice in *USA Today* regarding the Security Breach but claimed that no debit card pin numbers were compromised, a statement that is not accurate.

7. 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, in fact, "compromised."[6]

8. Defendant's security failures enabled the hackers to steal financial data from within Defendant's stores and subsequently make unauthorized purchases on customers' credit and debit cards and otherwise put Class members' PII at serious and ongoing risk. The hackers continue to use the PII they obtained as a result of Defendant's inadequate security to exploit and injure Class members across the United States.

9. Home Depot failed to uncover and disclose the extent of the Security Breach and notify its affected customers of the Breach in a timely manner. By failing to provide adequate notice, Home Depot prevented Class members from protecting themselves from the Security Breach.

---

[3] http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?module=Search&mabReward=relbias%3As (last visited December 18, 2014).

[4] *Id*.

[5] *Id*.

[6] https://corporate.homedepot.com/MediaCenter/Documents/Required%20Regulatory%20Notice.PDF(last visited December 18, 2014).

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

11. Home Depot disregarded Plaintiffs' 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, Plaintiffs' 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, Plaintiffs' and Class members' PII was compromised and stolen

12. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class (defined below), asserts claims for breach of implied contract and statutory violations of North Carolina law, and seeks injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

JURISDICTION AND VENUE

13. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the exclusive of interest and costs, and there are numerous class members who are citizens of States other than Defendant's state of citizenship.

14. This Court has personal jurisdiction over Defendant Home Depot in that Home Depot conducts substantial business in the State of North Carolina such that it has significant continuous and pervasive contacts with this State. Home Depot also maintains numerous locations and employees in North Carolina, including locations compromised in the Security Breach.

15. Venue is proper pursuant to 28 U.S.C. §1391 in that Plaintiffs reside or have their principal place of business in this District; many of the acts and transactions giving rise to this action occurred in this District; Defendant is authorized to conduct business in this District, has intentionally availed itself of the laws and markets within this District through distribution and sale of its products in this District, does substantial business in this District, and is subject to personal jurisdiction in this District.

PARTIES

Plaintiffs

16. Plaintiff John J. Hickey is a citizen of the State of North Carolina and currently resides in New Hanover County. Plaintiff made purchases with his Home Depot card at the Home Depot location in Wilmington, North Carolina, within the time period of the breach as stated by Defendant. As a result, Plaintiff John J. Hickey entered into an implied contract with

Home Depot for the adequate protection of his credit card information and had his sensitive financial and personal information exposed as a result of Defendant's inadequate security.

17. Plaintiff Kelly Toms is a citizen of the State of North Carolina and currently resides in New Hanover County. Plaintiff made purchases with her Visa debit card at the Home Depot location in Wilmington, North Carolina, within the time period of the breach as stated by Defendant. As a result, Plaintiff Kelly Toms entered into an implied contract with Home Depot for the adequate protection of her debit card information and had her sensitive financial and personal information exposed as a result of Defendant's inadequate security.

18. Plaintiff Suntzu Enterprises, Inc. is a North Carolina corporation with its principal place of business located in New Hanover County. Within the time period of the breach as stated by Defendant, employees of Plaintiff Suntzu Enterprises, Inc. made purchases at the Home Depot location in Wilmington, North Carolina, using a Home Depot card in the name of the company. As a result of these credit card transactions, Plaintiff Suntzu Enterprises, Inc. entered into an implied contract with Home Depot for the adequate protection of its credit card information and had sensitive financial information exposed as a result of Defendant's inadequate security.

19. Plaintiff Constructive Building Solutions, LLC is a North Carolina limited liability company with its principal place of business located in New Hanover County. Within the time period of the breach as stated by Defendant, employees of Constructive Building Solutions, LLC made 26 purchases at the Home Depot location in Wilmington, North Carolina, using a Visa credit card in the name of the company. As a result of these credit card transactions, Plaintiff Constructive Building Solutions, LLC entered into an implied contract with Home

Depot for the adequate protection of its credit card information and had sensitive financial information exposed as a result of Defendant's inadequate security

Defendant Home Depot

20. Home Depot U.S.A., Inc. is a Delaware corporation with its principal place of business in Atlanta, Georgia. Home Depot U.S.A., Inc. is a home improvement retailer.

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

22. Home Depot is the world's largest home improvement specialty retailer and fourth largest retailer in the United States, with stores in all 50 states, the District of Columbia, Puerto Rico, U.S. Virgin Islands, 10 Canadian provinces and Mexico.

FACTUAL ALLEGATIONS

The Data Breach

23. In what has become a nearly universal practice for retailers, Home Depot processes in-store debit and credit card payments for customer purchases.

24. On September 2, 2014, Home Depot's banking partners and law enforcement officials notified the retailer of a potential Security Breach involving the theft of its customers' credit card and debit card data.

25. 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 Corporation. According to security blogger Brian Krebs, a comparison of the

ZIP code data between the unique ZIPs represented on the rescator site and those of the Home Depot stores revealed a staggering 99.4 percent overlap.[7]

26. 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.[8]

27. After this news broke, Home Depot released an ambiguous statement buried on its corporate site – and not the Internet site visited by consumers – concerning the Security 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.[9]

28. To uncover further details, Defendant's forensics and security teams initiated an investigation in conjunction with outside IT security firms and the Secret Service. On September 8, 2014, Home Depot announced that its investigation had confirmed that customers' data was indeed compromised, and victims could include anyone who used a credit or debit card at *any* of the more than 2,200 Home Depot locations in the United States or Canada since April 2014.

29. 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

---

[7] http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/ (last visited December 18, 2014).

[8] http://online.wsj.com/articles/home-depot-tries-to-reassure-customers-about-possible-data-breach-1409743851 (last visited December 18, 2014).

[9] https://corporate.homedepot.com/mediacenter/pages/statement1.aspx (this language has since been removed and replaced with a confirmation of the data breach) (last visited December 18, 2014).

collects, including names, addresses, telephone numbers, mobile telephone numbers, driver's license numbers, bank account numbers, email addresses, computer IP addresses, and location information, were disclosed in the breach.[10]

30. According to one person briefed on the investigation, "the total number of credit [and debit] card numbers stolen at Home Depot could top 60 million,"[11] making this the largest data breach ever. The Attorneys General for California, Connecticut, Illinois, Iowa, and New York have already launched a joint probe into the Breach.[12]

31. 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 code of the Home Depot store from which the card was stolen.[13] This location information allows cyber thieves to quickly and more accurately locate the Social Security number and date of birth of cardholders, further increasing the risk of identity theft (above and beyond fraudulent credit and/or debit card transactions) for affected Home Depot customers.[14]

32. Even before Home Depot confirmed the Breach, criminals had already begun putting the stolen information to nefarious use. On September 2, 2014, banks began reporting evidence that Home Depot stores were the likely source of stolen card data that had surfaced at

---

[10] http://www.homedepot.com/c/Privacy_Security (last visited December 18, 2014).

[11] http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_r=0 (last visited December 18, 2014).

[12] http://www.newsweek.com/home-depot-data-breach-could-match-targets-biggest-ever-269286 (last visited December 18, 2014).

[13] http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit card-fraud/ (last visited December 18, 2014).

[14] *Id.*

rescator.cc, an underground cybercrime shop that also sold millions of cards stolen during Home Depot's recent security breach. Brian Krebs, the security blogger who first broke the story of the Breach, has reported that a comparison of the ZIP code data between the unique ZIPs represented on rescator.cc and those of the Home Depot stores revealed an overlap of more than 99.4%. According to Nicholas Weaver, a researcher at the International Computer Science Institute (ICSI) and at the University California, Berkeley, "[a] 99+ percent overlap in ZIP codes strongly suggests that this source is from Home Depot."

33. Customers' social security and date of birth information have already been pilfered and are being used to change the PIN numbers on stolen debit cards and to make ATM withdrawals directly from customers' accounts. On September 8, 2014, one large, West Coast bank reported losing more than $300,000 in two hours to PIN fraud on multiple debit cards that had all recently been used at Home Depot.[15] Other financial institutions have reported a steep increase in fraudulent ATM withdrawals on customer accounts in the week since the Security Breach was first reported.[16]

34. The Security Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. Home Depot grossly failed to comply with security standards and allowed its customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

[15] *Id.*
[16] *Id.*

35. 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.[17] Hackers had previously utilized BlackPOS in other recent cyber attacks, including last year's breach at Home Depot.[18] While many retailers, banks and card companies have responded to these recent breaches by adopting the use of microchips in U.S. credit and debit cards, technology that helps makes transactions more secure, Home Depot did not. In light of the breach, however, it has now announced that it plans to have chip-enabled checkout terminals at all of its U.S. stores by the end of 2014.[19]

36. Defendant's failure to comply with reasonable security standards provided Home Depot with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of its own customers – including Plaintiffs and Class members here – who have been subject to the Security Breach or otherwise have had their financial information placed at serious and ongoing risk.

37. Home Depot allowed widespread and systematic theft of its customers' financial information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' financial information.

Security Breaches Lead to Identity Theft

[17] http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/ (last visited December 18, 2014).

[18] *Id.*

[19] http://www.foxbusiness.com/markets/2014/09/04/home-depot-ceo-says-chip-enabled-terminals-will-be-activated-by-end-year/ (last visited December 18, 2014).

38. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying information ("PII") to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[20] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

39. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve.[21] Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[22]

40. A person whose PII has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [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.

---

[20] *See* http:///www.gao.gov/new.items/d07737.pdf (last visited December 18, 2014).

[21] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited December 18, 2014).

[22] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

41. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[23] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers and other PII directly on various Internet websites, making the information publicly available, just as they have done here.

The Monetary Value of Privacy Protections

42. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[24]

43. Though Commissioner Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[25]

---

[23] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* T. Soma, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009).

[24] *The Information Marketplace: Merging and Exchanging Consumer Data*, http://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited December 18, 2014).

[25] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited December 18, 2014) ("Web's Hot New Commodity: Privacy").

44. The FTC has also recognized that consumer data is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[26]

45. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from the surrender of their PII.[27] This business has created a new market for the sale and purchase of this valuable data.

46. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm, "when [retailers'] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[28]

---

[26] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited December 18, 2014).

[27] *You Want My Personal Data? Reward Me for It*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited December 18, 2014).

[28] Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited December 18, 2014); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

47. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use – two concerns at issue here – they valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use to between $7.98 and $11.68 per website.[29]

48. Indeed, each of the different elements of an individual's PII – email, date of birth, and usernames – all have a market for the purchase and trading of this information, which further illustrates that the *value* of such PII is staggeringly high.

49. As one prominent industry expert put the point: "Sign up with any service online, and it will almost certainly require you to supply an email address. In nearly all cases, the person who is in control of that address can reset the password of any associated services or accounts –merely by requesting a password reset email."[30]

50. For example, if hackers gain control of a person's Gmail account, they can reset the password to that person's FedEx shipping account or their United and Continental Airline accounts and have the new password sent to the compromised Gmail account. While the person figures out how to regain access with Google, the hackers can sell the victim's "Fedex.com, Continental.com and United.com accounts for USD $6."[31]

51. Both individual consumers and corporate/commercial consumers are at risk when hackers gain access to PII. Because business accounts have higher credit limits and more

[29] *Id.*

[30] http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/ (last visited December 18, 2014).

[31] *Id.*

purchases masking charges by scammers, "sophisticated identify thieves increasingly are targeting businesses because the payoffs are bigger." [32]

52. And while PII is worth money to hackers on even a pure elemental basis, in the aggregate, an individual's PII is even more lucrative.

Valuable PII Was Compromised And Is Now Being Used As a Result of the Security Breach

53. Among the data elements Home Depot collected and lost in its PII database were full name, address, zip code, and the last 4 digits of the individual's Social Security Number ("SSN") or Tax ID Number ("EIN") (the "4 Data Points").

54. Home Depot was quick to state (many times) in its press releases (the "FAQ"):

> *If I used my debit card at The Home Depot was my debit card PIN compromised/stolen?*
> At this time **we have no reason to believe debit card PINs were impacted** however, it is always a good idea to review your bank statements carefully and call your bank if you see any suspicious transactions. [33]

55. That statement is misleading *at best*, because the 4 Data Points can be used over the telephone to change the PIN number of a debit card and allow a hacker to withdraw money.

56. As Brian Krebs puts the point:

---

[32] http://www.businessweek.com/stories/2007-07-23/identity-theft-the-business-bust-outbusinessweek-business-news-stock-market-and-financial-advice (last visited December 18, 2014).

[33] https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf (last visited December 18, 2014) (emphasis added).

> Why do the thieves need Social Security and date of birth information? Countless banks in the United States let customers change their PINs with a simple telephone call, using an automated call-in system known as a Voice Response Unit (VRU). A large number of these VRU systems allow the caller to change their PIN provided they pass **three out of five security checks**. One is that the system checks to see if the call is coming from a phone number on file for that customer. It also requests the following four pieces of information:
>
> -the 3-digit code (known as a card verification value or CVV/CV2) printed on the back of the debit card;
> -the card's expiration date;
> -the customer's date of birth;
> -the last four digits of the customer's Social Security number.[34]

57. While the hackers may not have gotten PIN numbers from the Security Breach, they are certainly within the grasp of determined hacker and, thus, very much at risk, contrary to what Home Depot stated.

58. Home Depot also avers in its FAQ:

> *What can I do to protect myself?*
>
> It is always a good idea to review your payment card statements carefully and call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner.

59. This is federal law, not a policy of a company: the Fair Credit Billing Act (the "FCBA") and the Electronic Fund Transfer Act (the "EFTA"), 15 U.S.C. 1693 *et seq*., dictate this position. If an individual reports an ATM or debit card missing before unauthorized activity, pursuant to the EFTA, they are not responsible for any unauthorized transactions.

---

[34] http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/ (last visited December 18, 2014).

60. However, unlike credit cards, if there is unauthorized use of a debit or ATM card and the cardholder does not learn of the transactions and report them after 2 business days but less than 60 calendar days after the statement is sent, the cardholder is liable for unauthorized charges up to $500. After 60 days, this amount could be "All the money taken from your ATM/debit card account, and possibly more; for example, money in accounts linked to your debit account."[35] Thus, should someone make changes to a cardholder's debit card PIN or account information, they could lose everything in the account.

61. The SSN is a key data element for the hacker. It alone is worth several dollars per number on the black market. Krebs further explains: "I know of at least two very popular and long-running cybercrime stores that sell this (cardholder's Social Security Numbers) for a few dollars apiece. One of them even advertises the sale of this information on more than 300 million Americans."[36] That web site is called "SSN Finder" or https://ssnfinder.ru/, where individual SSNs are sold for $3 each. All that is necessary to get a SSN is first name, last name, full address with zip code.

62. With a name and address stolen from the Security Breach and a newly purchased, $3 social security number, an individual can file a tax return with the IRS electronically ("E-Filer"). If that E-Filer is due a refund, the refund amount can be instantly deposited in a

[35] http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards (last visited December 18, 2014).

[36] http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/ (last visited December 18, 2014).

bank account, and the E-Filer can direct the "IRS to direct deposit your refund into *your* account, your *spouse's* account or a *joint* account." It can also be split to several accounts.[37]

63. If a hacker with the name, address and a social security number of a taxpayer poses as the taxpayer and E-Files, the refund is sent to the account on the E-Filed form. Those funds are available within 24 hours of deposit by the Treasury. When the real taxpayer goes to file, he is told that his return is rejected as a duplicate return.

64. The link on the IRS web page labeled "Taxpayer Guide to Identity Theft" directs to a page that tells the taxpayer that an affidavit must be filed immediately. It is one of several arduous steps necessary for the taxpayer to correct his tax records.[38]

65. That web page identifies the problem: "Usually, an identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund. Generally, the identity thief will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season."

66. This is not a small problem: "Based on preliminary analysis, the Internal Revenue Service (IRS) estimates it paid $5.2 billion in fraudulent identity theft refunds in filing season 2013 while preventing an additional $24.2 billion (based on what it could detect)." [39]

67. In fact, in August of this year, the GAO submitted a report requested by Congress titled "Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud." It states the cost to the country, as well as the individual taxpayer: "In 2014, IRS has

---

[37] http://www.irs.gov/Individuals/Frequently-Asked-Questions-about-Splitting-Federal-Income-Tax-Refunds (last visited December 18, 2014).

[38] http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft (last visited December 18, 2014).

[39] http://www.networkworld.com/article/2687138/security0/to-fight-5-2b-worth-of-identity-theft-irs-may-need-to-change-the-way-you-file-taxes-get-refunds.html (last visited December 18, 2014).

approximately 3,000 people working on cases of IDT victims—more than twice the number of people working on these cases in 2011. In light of this, IRS recognized refund fraud and IDT as a major challenge affecting the agency in its recently issued strategic plan."[40]

68. A federal employer identification number ("EIN") is, in many respects, a Social Security number for a business. An EIN is a nine-digit number assigned by the IRS to identify a taxpayer's business account. The EIN used to uniquely identify the business and is required for commercial bank accounts, company credit card accounts and state and federal tax filing.[41]

69. Fraudulent accounts can be open in the name of a business with just the business name, an address, and the EIN. Additionally, an EIN can be used to obtain fraudulent tax refunds. [42]

70. In September 2013, the Treasury Inspector General for Tax Administration ("TIGTA") issued a report entitled "*Stolen and Falsely Obtained Employer Identification Numbers Are Used to Report False Income and Withholding*" detailing this growing problem.[43] The TIGTA found that 277,624 stolen EINs were used to report false income and withholding to the IRS resulting in fraudulent refunds totaling more than $2.2 billion being issued during the 2011 tax year alone.[44]

71. Based upon the analysis in this report, the TIGTA estimated that the IRS could issue over $11 billion in fraudulent tax returns over the next five years due to stolen EINs.[45]

---

[40] http://www.gao.gov/assets/670/665368.pdf (last visited December 18, 2014).

[41] http://www.businessidtheft.org/Education/BusinessIDTheftScams/BusinessEINandTaxFraud (last visited December 18, 2014).

[42] *Id.*

[43] http://www.treasury.gov/tigta/auditreports/2013reports/201340120fr.pdf

[44] *Id.*

[45] *Id.*

72. When the IRS begins comparing and matching reported wage and income information, often long after refunds have been issued, the unsuspecting business may face a deficiency in payroll taxes seemingly owed. As a result, the business and business owner face a difficult, costly and protracted and costly challenge to prove that a fraud has occurred.[46]

73. Given these facts, any company that transacts business with a consumer, whether an individual or a commercial entity, and then compromises the privacy of that consumer's PII, like Home Depot, has deprived that consumer of the full monetary value of the consumer's transaction with the company.

Damages Sustained By Plaintiffs and the Class

74. Because consumers place value in data privacy and security, they consider it when making purchasing decisions. Plaintiffs would not have made a purchase at Home Depot, or would not have paid as much as they did, had they known that Home Depot does not take all necessary precautions to secure its customers' 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.

75. A portion of the services purchased from Home Depot by Plaintiffs and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PII, including their credit and debit card information. Because Plaintiffs and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and the Class incurred actual monetary damages in that they overpaid for the services purchased

[46] http://www.businessidtheft.org/Education/BusinessIDTheftScams/BusinessEINandTaxFraud (last visited December 18, 2014).

from Home Depot or would not have made purchases at Home Depot had they known of Defendant's security failures.

76. Plaintiffs and the Class have suffered additional injury in fact and actual damages including monetary losses arising from unauthorized bank account withdrawals, fraudulent card payments, and/or related bank fees charged to their accounts.

77. After the Breach, Home Depot encouraged consumers to check their credit reports, place holds on their credit reports, and close any affected accounts. However, fraudulent use of cards might not be apparent for years. Therefore, consumers must expend considerable time taking these precautions for years to come.

78. Though Home Depot has offered one year of credit monitoring to affected customers, as Krebs notes, "credit monitoring services will do nothing to protect consumers from fraud on existing financial accounts – such as credit and debit cards – and they're not great at stopping new account fraud committed in your name."[47]

79. As a result of these activities, Plaintiffs and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Defendant's wrongful conduct, particularly given the incidents of actual misappropriation from Class members' financial accounts.

80. Plaintiffs and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiffs and the Class have been forced to expend to monitor their

[47] http://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/ (last visited December 18, 2014).

financial and bank accounts as a result of the Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

CLASS ACTION ALLEGATIONS

81. Plaintiffs bring this suit, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons residing in North Carolina who made an in-store purchase at a Home Depot location using a debit or credit card at any time from April 1, 2014 through September 9, 2014 (the "Class").

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

82. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

83. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, the security breach at issue affects over millions of customers of Home Depot. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from Defendant's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

84. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate

over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether Home Depot failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive financial information;

b. Whether Home Depot properly implemented its purported security measures to protect customer financial information from unauthorized capture, dissemination, and misuse;

c. Whether Defendant's conduct constitutes breach of an implied contract;

d. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief;

e. Whether Home Depot's conduct was unfair, deceptive and unconscionable;

f. Whether Home Depot violated North Carolina's Unfair and Deceptive Trade Practices Act; and,

g. Whether class members may obtain an injunctive relief against Home Depot.

85. Home Depot engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of himself and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action

86. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendant's uniform misconduct described above and were

thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Home Depot that are unique to Plaintiffs.

87. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seeks to represent, they have retained counsel competent and experienced in complex class action litigation, and will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

88. **Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Home Depot. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

89. **Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Home Depot has acted or refused to act on grounds generally applicable to Plaintiffs and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

90. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Home Depot, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS FOR RELIEF

COUNT I
Breach of Implied Contract

91. Plaintiffs hereby incorporate by reference the foregoing paragraphs of this Complaint as though set forth fully herein, and further state:

92. Customers who intended to make purchases at Defendant's retail locations with debit or credit cards were required to provide their card's magnetic strip data for payment verification.

93. In providing such financial data, Plaintiffs and the other members of the Class entered into an implied contract with Home Depot whereby Home Depot became obligated to reasonably safeguard Plaintiffs' and the other Class members' sensitive, non-public information.

94. Plaintiffs and the Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract.

95. Plaintiffs and Class members fully performed their obligations under the implied contracts with Home Depot.

96. Home Depot breached the implied contract with Plaintiffs and the other members of the Class by failing to take reasonable measures to safeguard their financial data and by failing to provide timely and accurate notice to them that their PII was compromised in and as a result of the Security Breach.

97. As a direct and proximate result of Home Depot's breaches of the implied contracts between Home Depot and Plaintiffs and Class members, Plaintiffs and Class members suffered and will continue to suffer damages including but not limited to loss of their financial information and loss of money and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

COUNT II
NEGLIGENCE

98. Plaintiffs hereby incorporate by reference the foregoing paragraphs of this Complaint as though set forth fully herein, and further state:

99. By accepting tender of Plaintiff's and Class members' debit and credit cards and obtaining the PII contained in the magnetic stripes of their cards, Home Depot had (and continues to have) a duty to exercise reasonable care in safeguarding the privacy of their PII to

prevent the unauthorized access of their PII and to otherwise undertake reasonable care in safeguarding and protecting the information from being compromised and/or stolen.

100. In addition, Home Depot had a duty to timely disclose the security breach and notify Plaintiff and Class Members' that their PII had been stolen.

101. Home Depot had a duty to put into place internal policies and procedures designed to protect and prevent the theft or dissemination of Plaintiff and Class Members' PII.

102. Home Depot, by failing to implement reasonable measures to protect the privacy of Plaintiff's and Class member's PII and to promptly notify them of the security breach, breached its duties to Plaintiff and the Class.

103. As a result of the above, Plaintiff and Class members have suffered damages and continue to be at serious risk of further harm from, among other things the unauthorized use of their credit and debit cards, and the further threats to the theft or unauthorized access to the PII in the hands of Defendant as Defendant has demonstrated an inability to safeguard their PII.

COUNT III
UNFAIR AND DECEPTIVE TRADE PRACTICES
N.C. GEN. STAT. § 75-1, *et seq*.

104. Plaintiffs hereby incorporate by reference the foregoing paragraphs of this Complaint as though set forth fully herein, and further state:

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

106. 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 UDTPA.

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

108. Plaintiff and Class Members are "consumers" "likely to be damaged" by Home Depot's ongoing deceptive trade practices.

109. Home Depot engaged in unfair and deceptive trade practices when it accepted its customers' PII and failed to adequately safeguard it.

110. Home Depot violated UDTPA by failing to properly implement adequate, commercially reasonable security measures to protect consumers' sensitive PII.

111. 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.

112. 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 Plaintiffs known truth about Home Depot's security procedures, they would not have made purchases at Home Depot, or would not have paid as much for them.

113. Home Depot's failure to disclose that it does not enlist industry standard security practices also constitutes an unfair business practice under the UDTPA. Home Depot's conduct is unethical, unscrupulous, and substantially injurious to Plaintiffs and the 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.

114. Home Depot also violated UDTPA by failing to immediately notify affected Plaintiff and Class Members of the nature and extent of the data breach.

115. Further, Home Depot violated UDTPA by violating the Identity North Carolina's Identity Theft Protection Act (ITPA), N.C.G.S. § 75-60, *et. seq*. (ITPA).

116. Home Depot violated ITPA by:

a. Failing to prevent the personal information of customers from falling into unauthorized hands;

b. Failing to properly dispose of all personal information of their customers; and,

c. Failing to provide adequate notice of the security breach to affected consumers upon discovery that their system had been compromised and personal information had been stolen.

117. 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.

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

119. Under UDPTA, 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.

120. 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.

121. Plaintiff accordingly requests that the Court enter an injunction requiring Home Depot to implement and maintain reasonable security procedures, 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, as well as the steps Home Depot's customers must take to protect themselves.

122. Plaintiff further requests that the Court requires Home Depot to identify and notify all members of the Class who have not yet been informed of the Security Breach, and to notify affected customers of any future data breaches by email within 24 hours of Home Depot's discovery of a breach or possible breach and by mail within 72 hours.

123. As a result of Home Depot's violations of the UDPTA, Plaintiffs and Class members have suffered injury in fact and lost money or property, as detailed in this Complaint. They purchased products or services they otherwise would not have purchased, or paid more for those products and services than they otherwise would have paid. Plaintiffs 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.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims in this complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in his favor and against Home Depot, as follows:

a. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representative and appointing the undersigned counsel as Class Counsel for the Class;

b. Ordering Home Depot to pay actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, to Plaintiffs and the other members of the Class;

c. Ordering Home Depot to pay for not less than three years of credit card monitoring services for Plaintiffs and the other members of the Class;

d. Ordering Home Depot to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;

e. Ordering Home Depot to disseminate individualized notice of the Security Breach to all Class members and to post notice of the Security Breach in all of its affected stores;

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

g. Ordering 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 compromised;

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

i. Ordering Home Depot to pay attorneys' fees and litigation costs to Plaintiffs and the other members of the Class;

j. For an award of attorney's fees and costs pursuant to N.C. Gen. Stat. § 75-16.1;

k. For treble damages pursuant to N.C. Gen. Stat § 75-16;

l. Ordering Home Depot to pay both pre- and post-judgment interest on any amounts awarded; and

m. Ordering such other and further relief as may be just and proper.

Dated: December 23, 2014

Respectfully submitted,

Counsel for Plaintiffs and the Proposed Class

/s/ Jean Sutton Martin
Jean Sutton Martin
North Carolina Bar No. 25703
Law Office of Jean Sutton Martin PLLC
2018 Eastwood Road Suite 225
Wilmington, NC 28403
Tel: (910) 292-6676
Fax: (888) 316-3485
Email: jean@jsmlawoffice.com

/s/ Joel R. Rhine
Joel R. Rhine
North Carolina Bar No. 16028
Rhine Law Firm, P.C.
1612 Military Cutoff Road Suite 300
Wilmington, NC 28403
Tel: (910) 772-9960
Fax: (910) 772-9062
Email: jrr@rhinelawfirm.com